100 XP

Introduction

1 minute

The traditional network security perimeter is changing as more companies move to either a hybrid cloud environment, with some resources located on-premises and some in the cloud, or a fully cloud-based network solution. Protection of your organization's assets, resources, and data is essential.

Threats can come from any direction: for instance, a Denial of Service attack on your organization's services, or a hacker trying to access your network by attempting to penetrate your firewall. Azure offers a wide array of configurable security tools that can be customized to give you the security and control to meet your organization's needs.

In this module, you explore many different services and features of Azure that can help protect your networks, assets, and resources, including DDoS protection, Azure Firewall, network security groups, and more. You'll also learn about Azure Key Vault and why you would use this feature to keep secrets safe.

After completing this module, you should be able to:

- **Describe Azure security capabilities for protecting your network.**
- **Describe Azure Bastion.**
- **Describe Azure Key Vault.**

Next unit: Describe Azure DDoS protection

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Azure DDoS protection

4 minutes

Any company, large or small, can be the target of a serious network attack. The nature of these attacks might be to make a statement, or because the attacker wanted a challenge.

Distributed Denial of Service attacks

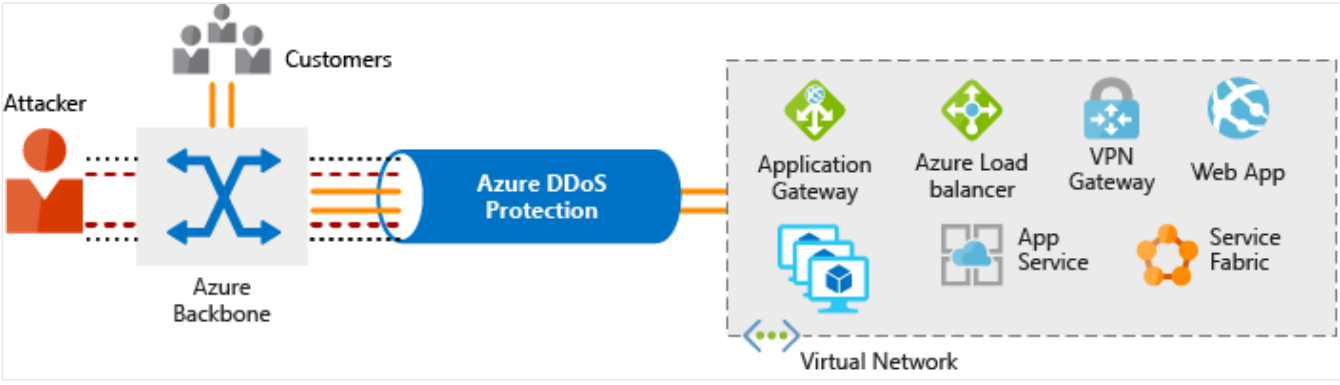
The aim of a Distributed Denial of Service (DDoS) attack is to overwhelm the resources on your applications and servers, making them unresponsive or slow for genuine users. A DDoS attack will usually target any public-facing device that can be accessed through the internet.

The three most frequent types of DDoS attack are:

- **Volumetric attacks: These are volume-based attacks that flood the network layer with seemingly legitimate traffic, overwhelming the available bandwidth. Legitimate traffic can't get through.**
- **Protocol attacks: Protocol attacks render a target inaccessible by exhausting server resources with false protocol requests that exploit weaknesses in layer 3 (network) and layer 4 (transport) protocols.**
- **Resource (application) layer attacks: These attacks target web application packets, to disrupt the transmission of data between hosts.**

What is Azure DDoS Protection?

The Azure DDoS Protection service is designed to help protect your applications and servers by analyzing network traffic and discarding anything that looks like a DDoS attack.



Azure DDoS Protection service protects at layer 3 (network layer) and layer 4 (transport layer). Key benefits provided include:

- **Always-on traffic monitoring: Your application traffic patterns are monitored 24 hours a day, 7 days a week, looking for indicators of DDoS attacks. Azure DDoS Protection instantly and automatically mitigates the attack, once it's detected. As part of the mitigation, traffic sent to the protected resource is redirected by the DDoS protection service and several checks are performed. Azure DDoS Protection drops attack traffic and forwards the remaining traffic to its intended destination. Within a few minutes of attack detection, you're notified using Azure Monitor metrics.**
- **Adaptive real time tuning: Intelligent traffic profiling learns your application's traffic over time, and selects and updates the profile that is the most suitable for your service. The profile adjusts as traffic changes over time.**
- **DDoS Protection telemetry, monitoring, and alerting: Azure DDoS Protection exposes rich telemetry via Azure Monitor. You can configure alerts for any of the Azure Monitor metrics that DDoS Protection uses. You can integrate logging with Azure Event Hubs, Azure Monitor logs, and Azure Storage for advanced analysis via the Azure Monitor Diagnostics interface.**

Azure DDoS Protection supports two tier types, DDoS IP Protection and DDoS Network Protection. The tier is configured in the Azure portal when you configure Azure DDoS Protection.

- **DDoS Network Protection: The DDoS Network Protection service (available as a SKU), combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It's automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes.**
- **DDoS IP Protection: DDoS IP Protection is a pay-per-protected IP model. DDoS IP Protection contains the same core engineering features as DDoS Network Protection, but differs in that it doesn't include the value-added services such as DDoS rapid response support, cost protection, and discounts on Web Application Firewall (WAF) that are part of DDoS Network Protection. For a complete listing of the features and corresponding tiers, see About Azure DDoS Protection tier Comparison**

A common question that is often raised is why consider adding DDos Protection services if services running on Azure are inherently protected by the default infrastructure-level DDoS protection? The reason is because the protection that safeguards the infrastructure has a higher threshold than most applications have the capacity to handle, and doesn't

provide telemetry or alerting. So while traffic volume may be perceived as harmless by the platform, it can be devastating to the application that receives it. By onboarding to the Azure DDoS Protection Service, the application gets dedicated monitoring to detect attacks and application specific thresholds. A service will be protected with a profile that is tuned to its expected traffic volume, providing a tighter defense against DDoS attacks.

As mentioned, earlier, Azure DDos Protection protects at layer 3 and layer 4. For web applications protection at layer 7 (the application layer), you need to add protection at the application layer using a Web Application Firewall (WAF) offering, described in a subsequent unit of this module.

Next unit: Describe Azure Firewall

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

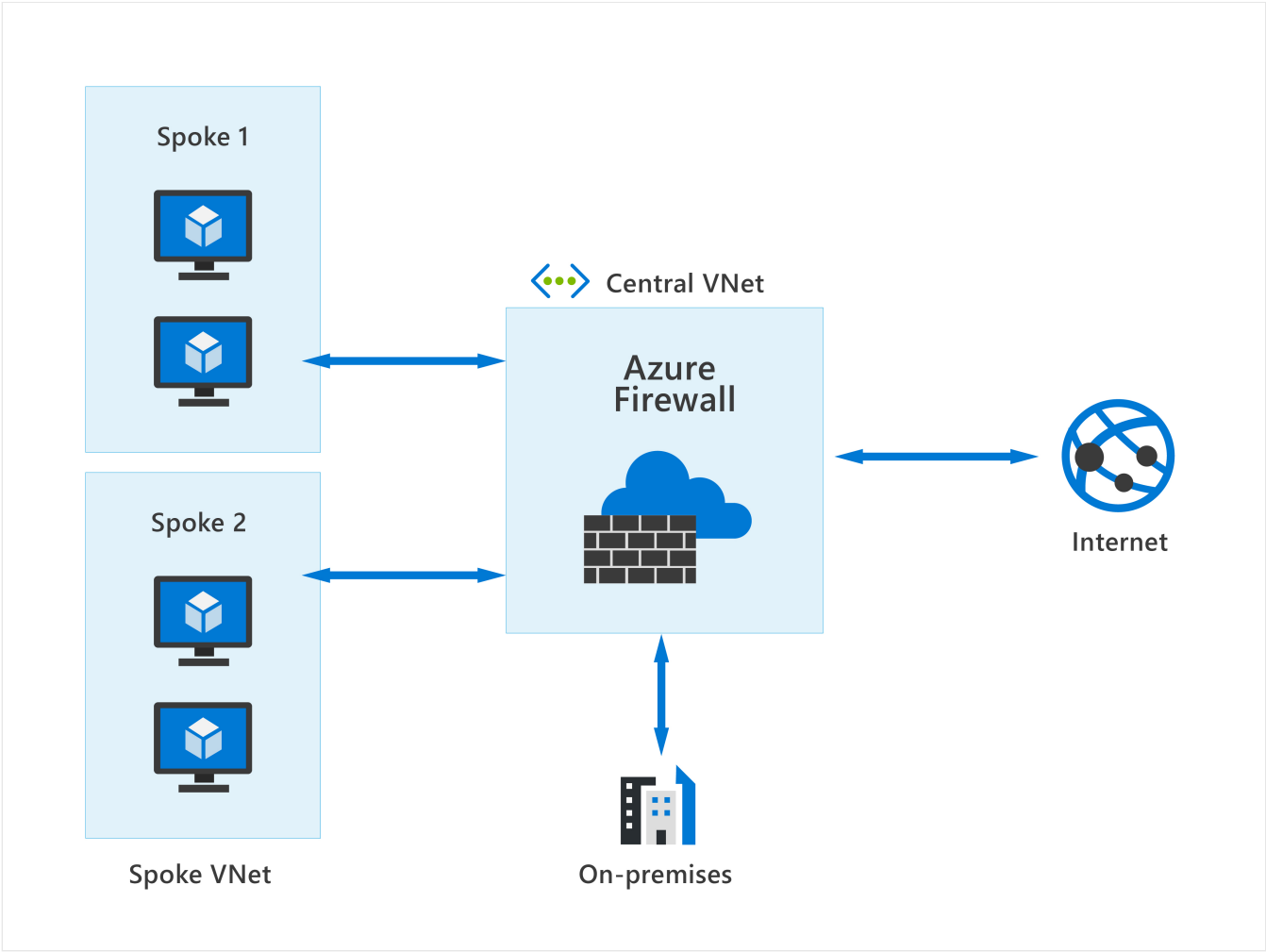
100 XP

Describe Azure Firewall

2 minutes

Azure Firewall is a managed, cloud-based network security service that provides threat protection for your cloud workloads and resources running in Azure.

You can deploy Azure Firewall on any virtual network but the best approach is to use it on a centralized virtual network. All your other virtual and on-premises networks will then route through it. The advantage of this model is the ability to centrally exert control of network traffic for all your VNets across different subscriptions.



With Azure Firewall, you can scale up the usage to accommodate changing network traffic flows, so you don't need to budget for peak traffic. Network traffic is subjected to the configured firewall rules when you route it to the firewall as the subnet default gateway.

Key features of Azure Firewall

Azure Firewall is offered in three SKUs: Standard, Premium, and Basic. The list that follows provides a list of some of the key features that are included across all Azure Firewall SKUs.

- **Built-in high availability and availability zones: High availability is built in so there's nothing to configure. Also, Azure Firewall can be configured to span multiple availability zones for increased availability.**
- **Network and application level filtering: Use IP address, port, and protocol to support fully qualified domain name filtering for outbound HTTP(s) traffic and network filtering controls.**
- **Outbound SNAT and inbound DNAT to communicate with internet resources: Translate the private IP address of network resources to an Azure public IP address (source network address translation or SNAT) to identify and allow traffic originating from the virtual network to internet destinations. Similarly, inbound internet traffic to the firewall public IP address is translated (Destination Network Address Translation or DNAT) and filtered to the private IP addresses of resources on the virtual network.**
- **Multiple public IP addresses: These addresses can be associated with Azure Firewall.**
- **Threat intelligence: Threat intelligence-based filtering can be enabled for your firewall to alert and deny traffic from/to known malicious IP addresses and domains.**
- **Integration with Azure Monitor: Integrated with Azure Monitor to enable collecting, analyzing, and acting on telemetry from Azure Firewall logs.**

Detailed information of the features included for each of the available SKUs (standard, premium, and basic) is provided in the Learn more section in the summary and resources unit.

Next unit: Describe Web Application Firewall

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

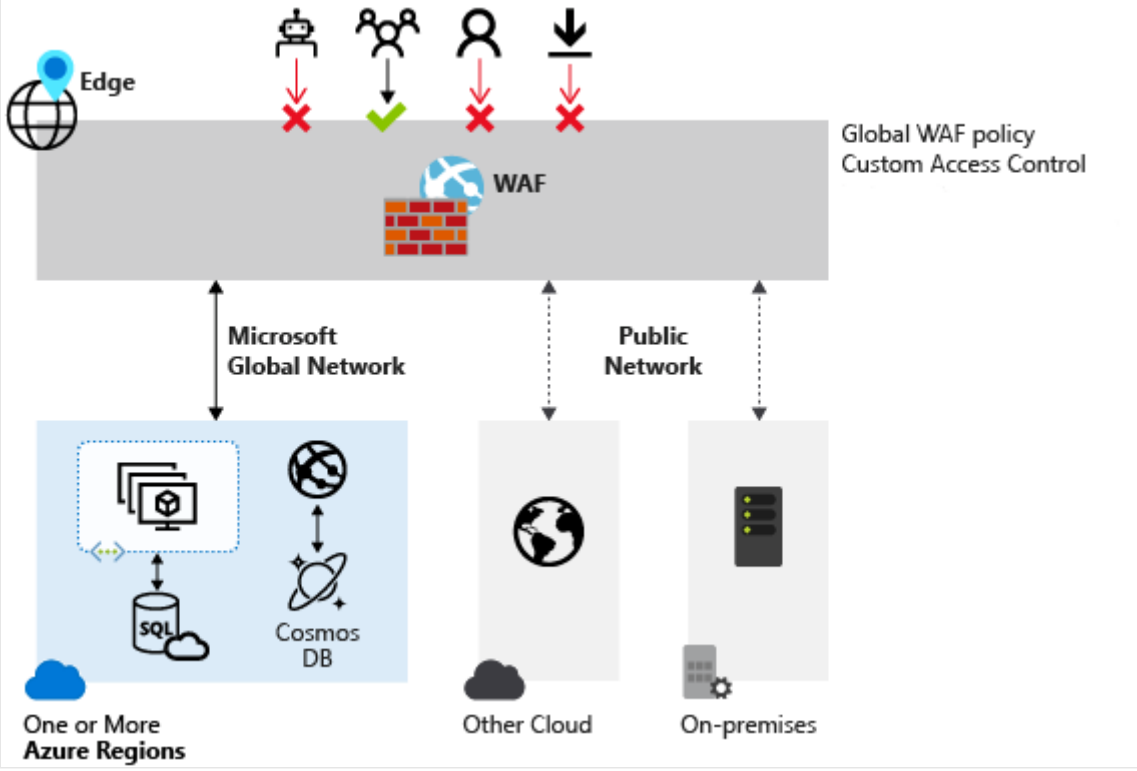
Describe Web Application Firewall

1 minute

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. Preventing such attacks in application code is challenging. It can require rigorous maintenance, patching, and monitoring.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. A centralized WAF helps make security management simpler, improves the response time to a security threat, and allows patching a known vulnerability in one place, instead of securing each individual web application. A WAF also gives application administrators better assurance of protection against threats and intrusions.

Among the types of threats that WAF can protect against are distributed denial of service (DDoS) attacks that occur at the application layer. While Azure DDoS Protection services protect customers against DDoS attacks that can occur at the network and transport layers, Azure WAF protects web applications against application-layer DDoS attacks, such as HTTP Floods. These defenses can prevent attackers from reaching your application and affecting your application's availability and performance.



Next unit: Describe network segmentation in Azure

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe network segmentation in Azure

2 minutes

Segmentation is about dividing something into smaller pieces. An organization, for example, will typically consist of smaller business groups such as human resources, sales, customer service, and more. In an office environment, it's common to see each business group have their own dedicated office space, while members of the same group share an office. This enables members of the same business group to collaborate, while maintaining separation from other groups to address the confidentiality requirements of each business.

The same concept applies with corporate IT networks. The main reasons for network segmentation are:

- **The ability to group related assets that are a part of (or support) workload operations.**
- **Isolation of resources.**
- **Governance policies set by the organization.**

Network segmentation also supports the Zero Trust model and a layered approach to security that is part of a defense in depth strategy.

Assume breach is a principle of the Zero Trust model so the ability to contain an attacker is vital in protecting information systems. When workloads (or parts of a given workload) are placed into separate segments, you can control traffic from/to those segments to secure communication paths. If one segment is compromised, you'll be able to better contain the impact and prevent it from laterally spreading through the rest of your network.

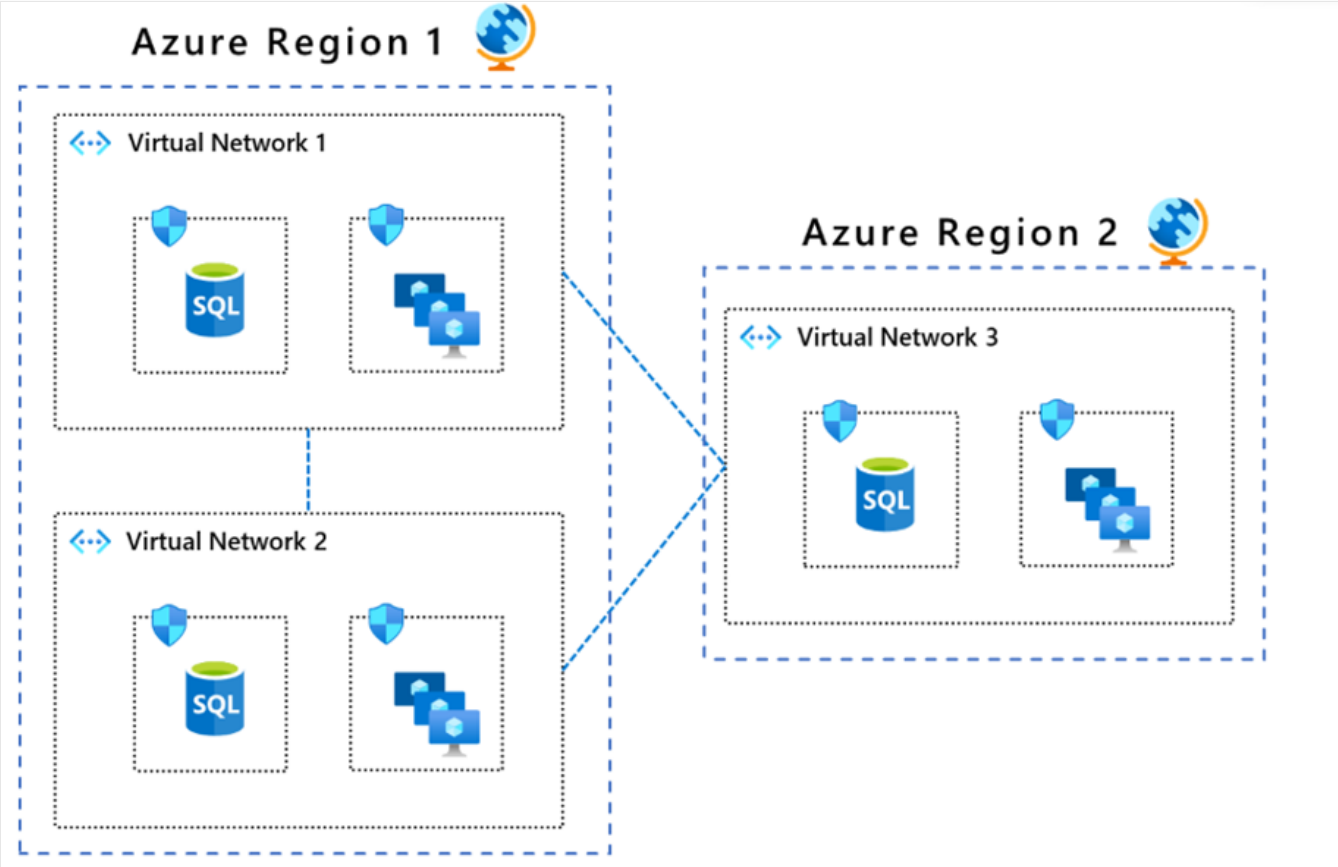
Network segmentation can secure interactions between perimeters. This approach can strengthen an organization's security posture, contain risks in a breach, and stop attackers from gaining access to an entire workload.

Azure Virtual Network

Azure Virtual Network (VNet) is the fundamental building block for your organization's private network in Azure. A virtual network is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Azure virtual network enables organizations to segment their network. Organizations can create multiple virtual networks per region per subscription, and multiple smaller networks (subnets) can be created within each virtual network.

VNets provide network level containment of resources with no traffic allowed across VNets or inbound to the virtual network, by default. Communication needs to be explicitly provisioned. This enables more control over how Azure resources in a virtual network communicate with other Azure resources, the internet, and on-premises networks.



Next unit: Describe Azure Network Security groups

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

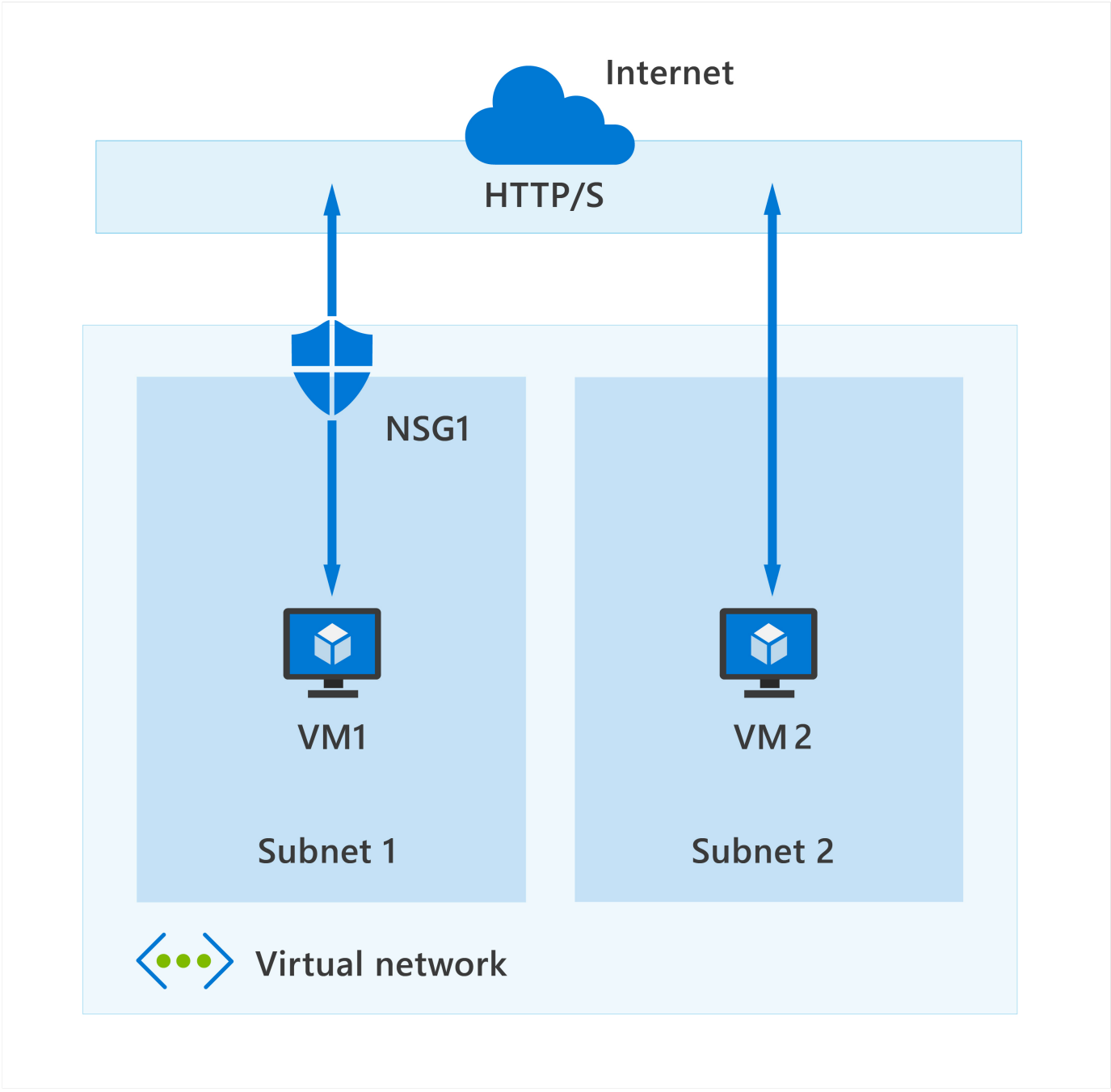
100 XP

Describe Azure Network Security groups

6 minutes

Network security groups (NSGs) let you filter network traffic to and from Azure resources in an Azure virtual network; for example, a virtual machine. An NSG consists of rules that define how the traffic is filtered. You can associate only one network security group to each virtual network subnet and network interface in a virtual machine. The same network security group, however, can be associated to as many different subnets and network interfaces as you choose.

In the highly simplified diagram that follows, you can see an Azure virtual network with two subnets that are connected to the internet, and each subnet has a virtual machine. Subnet 1 has an NSG assigned to it that's filtering inbound and outbound access to VM1, which needs a higher level of access. In contrast, VM2 could represent a public-facing machine that doesn't require an NSG.



Inbound and outbound security rules

An NSG is made up of inbound and outbound security rules. NSG security rules are evaluated by priority using five information points: source, source port, destination, destination port, and protocol to either allow or deny the traffic. By default, Azure creates a series of

rules, three inbound and three outbound rules, to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

Each rule specifies one or more of the following properties:

- **Name: Every NSG rule needs to have a unique name that describes its purpose. For example, AdminAccessOnlyFilter.**
- **Priority: Rules are processed in priority order, with lower numbers processed before higher numbers. When traffic matches a rule, processing stops. This means that any other rules with a lower priority (higher numbers) won't be processed.**
- **Source or destination: Specify either individual IP address or an IP address range, service tag (a group of IP address prefixes from a given Azure service), or application security group. Specifying a range, a service tag, or application security group, enables you to create fewer security rules.**
- **Protocol: What network protocol will the rule check? The protocol can be any of: TCP, UDP, ICMP or Any.**
- **Direction: Whether the rule should be applied to inbound or outbound traffic.**
- **Port range: You can specify an individual or range of ports. Specifying ranges enables you to be more efficient when creating security rules.**
- **Action: Finally, you need to decide what will happen when this rule is triggered.**

As an example, the table that follows shows the default inbound rules, which are included in all NSGs. For this example, assume no other inbound rules have been defined for this NSG.

Name	Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
AllowVNetInBound	65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow
AllowAzureLoadBalancerInBound	65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow
DenyAllInBound	65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

- **The AllowVNetInBound rule is processed first as it has the lowest priority value. Recall that rules with the lowest priority value get processed first. This rule allows traffic from any Virtual Network (as defined by the VirtualNework service tag) on any port to any Virtual Network on any port, using any protocol. If a match is found for this rule, then no other rules are processed. If no match is found, then the next rule gets processed.**
- **The AllowAzureLoadBalancerInBound rule is processed second, as its priority value is higher than the AllowVNetInBound rule. This rule allows traffic from any Azure Load Balancer (as defined by the AzureLoadBalancer service tag) on any port to any IP address on any port, using any protocol. If a match is found for this rule, then no other rules are processed. If no match is found, then the next rule gets processed.**
- **The last rule in this NSG is the DenyAllInBound rule. This rule denies all traffic from any source IP address on any port to any other IP address on any port, using any protocol.**

In summary, any virtual network subnet or network interface card to which this NSG is assigned will only allow inbound traffic from an Azure Virtual Network or an Azure load balancer. All other inbound network traffic is denied. Although not shown in this example, there are also three default outbound rules that are included in all NSGs. You can't remove the default rules, but you can override them by creating new rules with higher priorities (lower priority value).

What is the difference between Network Security Groups (NSGs) and Azure Firewall?

Now that you've learned about both Network Security Groups and Azure Firewall, you may be wondering how they differ, as they both protect Virtual Network resources. The Azure Firewall service complements network security group functionality. Together, they provide better "defense-in-depth" network security. Network security groups provide distributed network layer traffic filtering to limit traffic to resources *within* virtual networks in each subscription. Azure Firewall is a fully stateful, centralized network firewall as-a-service, which provides network and application-level protection *across* different subscriptions and virtual networks.

Next unit: Describe Azure Bastion

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Azure Bastion

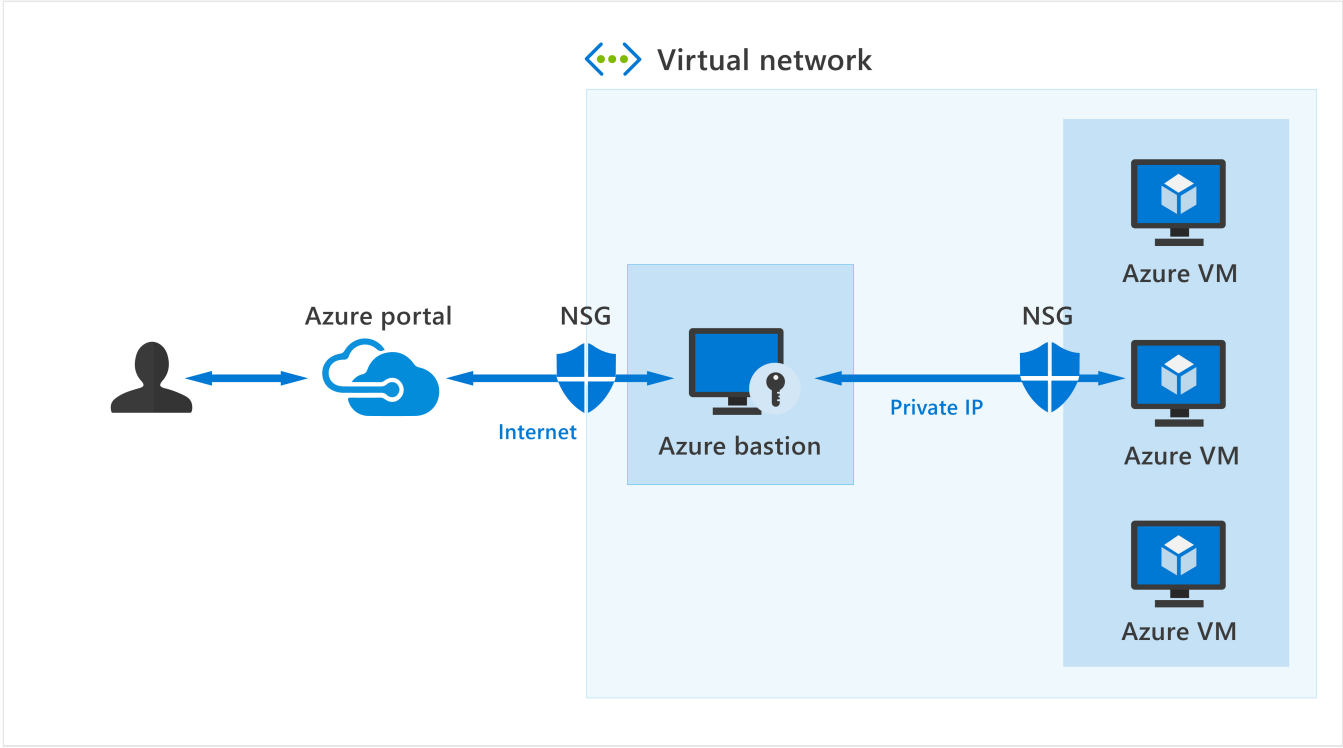
6 minutes

Let's assume you've set up multiple virtual networks that use a combination of NSGs and Azure Firewalls to protect and filter access to the assets and resources, including virtual machines (VMs). You're now protected from external threats, but need to allow your developers and data scientist, who are working remotely, direct access to those VMs.

In a traditional model, you'd need to expose the Remote Desktop Protocol (RDP) and/or Secure Shell (SSH) ports to the internet. These protocols can be used to gain remote access to your VMs. This process creates a significant surface threat that can be exploited by attackers who actively hunt accessible machines with open management ports, like RDP or SSH. When a VM is successfully compromised, it's used as the entry point to attack further resources within your environment.

Azure Bastion

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal using Transport Layer Security (TLS). When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.



Bastion provides secure RDP and SSH connectivity to all VMs in the virtual network, and peered virtual networks, in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Bastion deployment is per virtual network with support for virtual network peering, not per subscription/account or virtual machine. Once you provision the Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same VNet, and peered VNets.

Key benefits of Azure Bastion

The following are key benefits of Azure Bastion:

- **RDP and SSH directly in Azure portal: You get to the RDP and SSH session directly in the Azure portal, using a single-click experience.**
- **Remote session over TLS and firewall traversal for RDP/SSH: From the Azure portal, a connection to the VM, will open an HTML5 based web client that is automatically streamed to your local device. You'll get your Remote Desktop Protocol (RDP) and Secure Shell (SSH) to traverse the corporate firewalls securely. The connection is made secure by using the Transport Layer Security (TLS) protocol to establish encryption.**
- **No Public IP required on the Azure VM: Azure Bastion opens the RDP/SSH connection to your Azure virtual machine using private IP on your VM. You don't need a public IP.**

- **No hassle of managing NSGs: A fully managed platform PaaS service from Azure that's hardened internally to provide secure RDP/SSH connectivity. You don't need to apply any NSGs on an Azure Bastion subnet.**
- **Protection against port scanning: Because you don't need to expose your virtual machines to the internet, your VMs are protected against port scanning by rogue and malicious users located outside your virtual network.**
- **Hardening in one place to protect against zero-day exploits: Azure Bastion is a fully platform-managed PaaS service. Because it sits at the perimeter of your virtual network, you don’t need to worry about hardening each virtual machine in the virtual network. The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.**

Use Azure Bastion to establish secure RDP and SSH connectivity to your virtual machines in Azure.

Azure Bastion has two available SKUs, Basic and Standard. For more information on features available in the available SKUs, see the linked documentation in the Learn more section of the summary and resources unit.

Next unit: Describe Azure Key Vault

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Azure Key Vault

3 minutes

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

Azure Key Vault helps solve the following problems:

- **Secrets management. You can use Key Vault to store securely and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.**
- **Key management. You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.**
- **Certificate management. Key Vault lets you provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates for use with Azure and internally connected resources.**

Azure Key Vault has two service tiers: Standard, which encrypts with a software key, and a Premium tier, which includes hardware security module (HSM)-protected keys.

Why use Key Vault?

Centralize application secrets. Centralizing storage of application secrets in Azure Key Vault allows you to control their distribution and greatly reduces the chances that secrets may be accidentally leaked. When application developers use Key Vault, they no longer need to store security information as part of the code in their application. Instead, the application can securely access the information it needs by using a Key Vault object identifier that uniquely identifies the object within the Key Vault. Key Vault object identifiers are URLs that allow the application to retrieve specific versions of a secret. There's no need to write custom code to protect any of the secret information stored in Key Vault.

Examples of the URL format for a standard tier Azure Key Vault object identifier and the premium tier managed HSM are as follows:

- **For standard tier vaults: https://{vault-name}.vault.azure.net/{object-type}/{object-name}/{object-version}**

- **For Managed HSM: https://{hsm-name}.managedhsm.azure.net/{object-type}/{object-name}/{object-version}**

Securely store secrets and keys. Access to a key vault requires proper authentication and authorization before a caller (user or application) can get access. Authentication establishes the identity of the caller, while authorization determines the operations that they're allowed to perform.

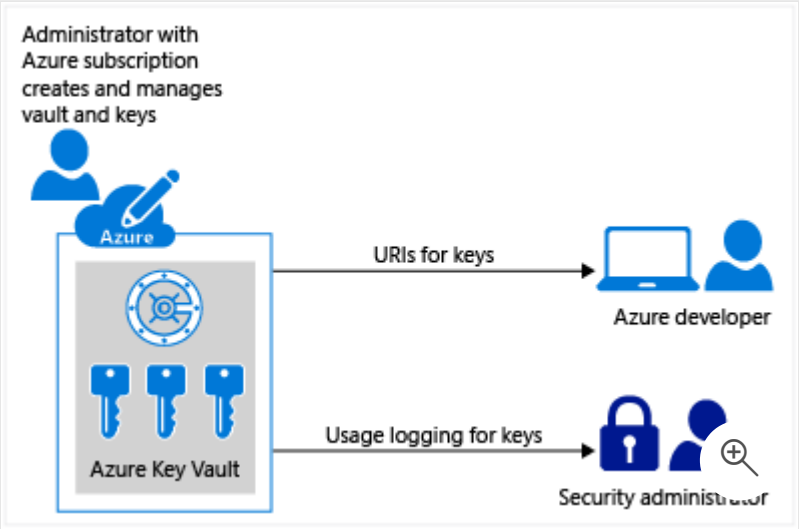
Authentication is done via Microsoft Entra. Authorization may be done via Azure role-based access control (Azure RBAC) or Key Vault access policy.

Azure Key Vault is designed so that Microsoft doesn't see or extract your data.

Monitor access and use. Once you've created a couple of Key Vaults, you can monitor activity by enabling logging for your vaults. You have control over your logs and you may secure them by restricting access and you may also delete logs that you no longer need.

Simplified administration of application secrets. Azure Key Vault simplifies the administration that would typically be required to secure your application secrets, including:

- **Replicating the contents of your Key Vault within a region and to a secondary region. Data replication ensures high availability and takes away the need of any action from the administrator to trigger the failover.**
- **Providing standard Azure administration options via the portal, Azure CLI and PowerShell.**
- **Automating certain tasks on certificates that you purchase from Public Certificate Authorities (CAs), such as enrollment and renewal.**



In addition, Azure Key Vaults allow you to segregate application secrets. Applications may access only the vault that they're allowed to access, and they can be limited to only

perform specific operations. You can create an Azure Key Vault per application and restrict the secrets stored in a Key Vault to a specific application and team of developers.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

Summary and resources

1 minute

The traditional network security perimeter protects your organization's assets, resources, where data is essential. Azure offers a wide range of configurable security tools that are customized to give the security and control to meet your organization's needs.

You've explored the different service offerings provided by Azure, including DDoS protection, Azure Firewall, network security groups, and Azure Bastion to protect access to your systems. You now understand the reasons to use Azure Key Vault.

Without these security tools, your organization would be vulnerable to data theft, unable to respond swiftly to malicious attacks on your web and data services, and wouldn't meet your security obligations.

Now that you've completed this module, you should be able to:

- **Describe Azure security capabilities for protecting your network.**
- **Describe Azure Bastion.**
- **Describe Azure Key Vault.**

Learn more

To find out more about any of the topics covered in this module, go to:

- **Azure DDoS Protection overview**
- **Azure DDoS Protection pricing page**
- **Azure Firewall**
- **Web Application firewall**
- **Network Security Groups**
- **Azure Bastion**
- **About Azure Key Vault**

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

As more companies move their assets and resources into the cloud, keeping them safe is a primary consideration for all IT and security departments. Cybercrime is a multi-billion-dollar business. Failure to protect your organization can be costly because of loss of data and reputation.

Microsoft Azure offers a suite of threat protection and detection systems to minimize and mitigate threats across your whole estate and improve the overall cloud security posture.

In this module, you'll learn about cloud security posture management (CSPM), explore the capabilities of Microsoft Defender for Cloud, including secure score. You will also learn about the enhanced security capabilities of Microsoft Defender for Cloud. Finally, you'll learn about the Microsoft cloud security benchmark and security baseline in Azure.

After completing this module, you'll be able to:

- **Describe cloud security posture management.**
- **Describe the capabilities of Microsoft Defender for Cloud**
- **Understand the Microsoft cloud security benchmark and security baseline in Azure.**

Next unit: Describe Cloud security posture management

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Cloud security posture management

2 minutes

Cloud-based systems are continually evolving and changing as companies move away from on-premises to the cloud. This move makes it difficult for any IT department to know if your data, assets, and resources are as fully protected as they used to be. Even a small misconfiguration of a new feature can increase the attack surface available for cybercriminals to exploit.

Cloud security posture management (CSPM) is a relatively new class of tools designed to improve your cloud security management. It assesses your systems and automatically alerts security staff in your IT department when a vulnerability is found. CSPM uses tools and services in your cloud environment to monitor and prioritize security enhancements and features.

CSPM uses a combination of tools and services:

- **Zero Trust-based access control: Considers the active threat level during access control decisions.**
- **Real-time risk scoring: To provide visibility into top risks.**
- **Threat and vulnerability management (TVM): Establishes a holistic view of the organization's attack surface and risk and integrates it into operations and engineering decision-making.**
- **Discover risks: To understand the data exposure of enterprise intellectual property, on sanctioned and unsanctioned cloud services.**
- **Technical policy: Apply guardrails to audit and enforce the organization's standards and policies to technical systems.**
- **Threat modeling systems and architectures: Used alongside other specific applications.**

The main goal for a cloud security team working on posture management is to continuously report on and improve the organization's security posture by focusing on disrupting a potential attacker's return on investment (ROI).

The function of CSPM in your organization might be spread across multiple teams, or there may be a dedicated team. CSPM can be useful to many teams in your organization:

- **Threat intelligence team**

- **Information technology**
- **Compliance and risk management teams**
- **Business leaders and SMEs**
- **Security architecture and operations**
- **Audit team**

Use CSPM to improve your cloud security management by assessing the environment, and automatically alerting security staff for vulnerabilities.

Next unit: Describe Microsoft Defender for Cloud

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Defender for Cloud

6 minutes

Microsoft Defender for Cloud is a tool for security posture management and threat protection. It strengthens the security posture of your cloud resources, and with its integrated Microsoft Defender plans, Defender for Cloud protects workloads running in Azure, hybrid, and other cloud platforms.

Microsoft Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- **Continuously assess - Know your security posture, identify and track vulnerabilities.**
- **Secure - Harden all connected resources and services.**
- **Defend - Detect and resolve threats to resources, workloads, and services.**

The features of Microsoft Defender for Cloud, that deliver on these requirements, cover two broad pillars of cloud security: cloud security posture management and cloud workload protection.

Cloud security posture management (CSPM)

In Microsoft Defender for Cloud, the posture management features provide:

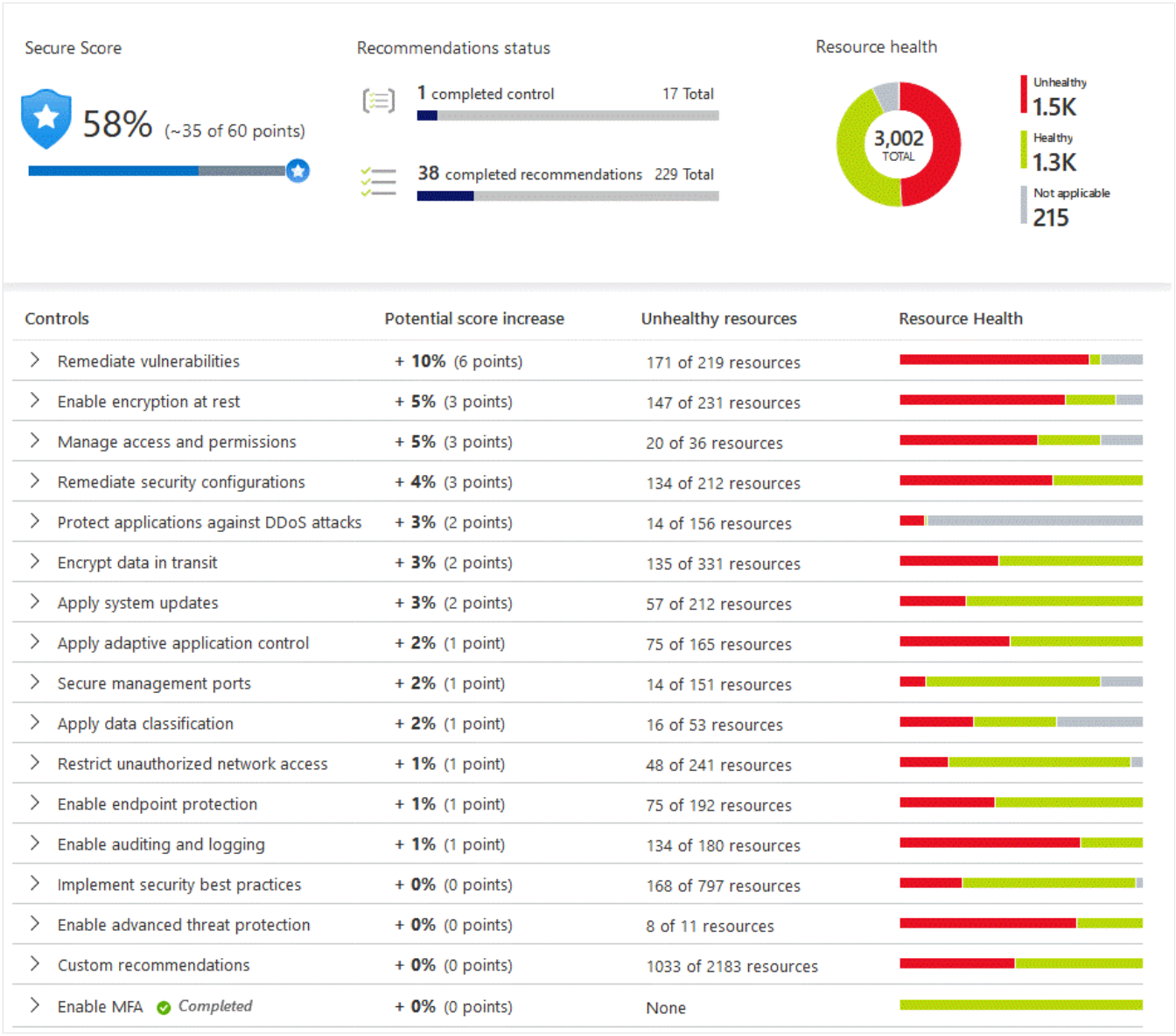
- **Visibility - to help you understand your current security situation**
- **Hardening guidance - to help you efficiently and effectively improve your security**

Visibility and hardening recommendations

The central feature in Microsoft Defender for Cloud that enables you to achieve those goals is secure score. Microsoft Defender for Cloud continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

Microsoft Defender for Cloud also provides hardening recommendations based on any identified security misconfigurations and weaknesses. Recommendations are grouped into security controls. Each control is a logical group of related security recommendations, and reflects your vulnerable attack surfaces. Your score only improves when you remediate all of the recommendations for a single resource within a control.

Use these security recommendations to strengthen the security posture of your organization's Azure, hybrid, and multicloud resources.



The following interactive click-through demonstrates how you use secure score and the hardening recommendations in Microsoft Defender for Cloud. Select the image below to get started and follow the prompts on the screen.

Cloud workload protection (CWP)

The second pillar of cloud security is cloud workload protection. Through cloud workload protection capabilities, Microsoft Defender for Cloud is able to detect and resolve threats to resources, workloads, and services. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads. These are described in the next unit.

Next unit: Describe the enhanced security of Microsoft Defender for Cloud

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the enhanced security of Microsoft Defender for Cloud

5 minutes

Microsoft Defender for Cloud is offered in two modes:

- **Microsoft Defender for Cloud (Free) - Microsoft Defender for Cloud is enabled for free on all your Azure subscriptions. Using this free mode provides the secure score and its related features: security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.**
- **Microsoft Defender for Cloud with enhanced security features - Enabling enhanced security extends the capabilities of the free mode to workloads running in Azure, hybrid, and other cloud platforms, providing unified security management and threat protection across your workloads. Cloud workload protections are delivered through integrated Microsoft Defender plans, specific to the types of resources in your subscriptions and provide enhanced security features for your workloads.**

Defender plans

Microsoft Defender for Cloud includes a range of advanced intelligent protections for your workloads. The workload protections are provided through Microsoft Defender plans specific to the types of resources in your subscriptions. The Microsoft Defender for Cloud plans you can select from are:

- **Microsoft Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.**
- **Microsoft Defender for App Service identifies attacks targeting applications running over App Service.**
- **Microsoft Defender for Storage detects potentially harmful activity on your Azure Storage accounts.**
- **Microsoft Defender for SQL secures your databases and their data wherever they're located.**
- **Microsoft Defender for Kubernetes provides cloud-native Kubernetes security environment hardening, workload protection, and run-time protection.**
- **Microsoft Defender for container registries protects all the Azure Resource Manager based registries in your subscription.**

- **Microsoft Defender for Key Vault is advanced threat protection for Azure Key Vault.**
- **Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization.**
- **Microsoft Defender for DNS provides an additional layer of protection for resources that use Azure DNS's Azure-provided name resolution capability.**
- **Microsoft Defender for open-source relational protections brings threat protections for open-source relational databases.**

These different plans can be enabled separately and will run simultaneously to provide a comprehensive defense for compute, data, and service layers in your environment.

Enhanced security features

Microsoft Defender plans specific to the types of resources in your subscriptions provide enhanced security features for your workloads. Listed below are some of the enhanced security features.

- **Comprehensive endpoint detection and response - Microsoft Defender for servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR).**
- **Vulnerability scanning for virtual machines, container registries, and SQL resources - Easily deploy a scanner to all of your virtual machines. View, investigate, and remediate the findings directly within Microsoft Defender for Cloud.**
- **Multicloud security - Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features.**
- **Hybrid security – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.**
- **Threat protection alerts - Monitor networks, machines, and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.**
- **Track compliance with a range of standards - Microsoft Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark. When you enable the enhanced security features, you can apply a range of other industry**

standards, regulatory standards, and benchmarks according to your organization's needs. Add standards and track your compliance with them from the regulatory compliance dashboard.

- **Access and application controls - Block malware and other unwanted applications by applying machine learning powered recommendations adapted to your specific workloads to create allowlists and blocklists. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs. Access and application controls drastically reduce exposure to brute force and other network attacks.**

Additional benefits include threat protection for the resources connected to the Azure environment and container security features, among others. Some features may be associated with specific Defender plans for specific workloads.

Next unit: Describe the Microsoft cloud security benchmark and security baselines for Azure

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the Microsoft cloud security benchmark and security baselines for Azure

5 minutes

> **Note**
>
> **Microsoft cloud security benchmark is the successor of Azure Security Benchmark (ASB), which was rebranded in October 2022. It is currently in public preview.**

New services and features are released daily in Azure, developers are rapidly publishing new cloud applications built on these services, and attackers are always seeking new ways to exploit misconfigured resources.

The Microsoft cloud security benchmark and security baselines for Azure, which are closely related, help organizations secure their cloud solutions on Azure.

Microsoft cloud security benchmark

Microsoft has found that using security benchmarks can help organizations quickly secure their cloud deployments and reduce risk to their organization.

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multicloud environment.

The best way to understand the Microsoft cloud security benchmark is to view it on GitHub Microsoft_cloud_security_benchmark . Spoiler alert, it's an excel spreadsheet. Some of the key pieces of information in MCSB V1 are:

- **ID - Each line item in the MCSB has an identifier that maps to a specific recommendation.**
- **Control domain - A control is a high-level description of a feature or activity that needs to be addressed and isn't specific to a technology or implementation. MCSB control domains include network security, data protection, identity management, privileged access, incident response, endpoint security to name just a few.**

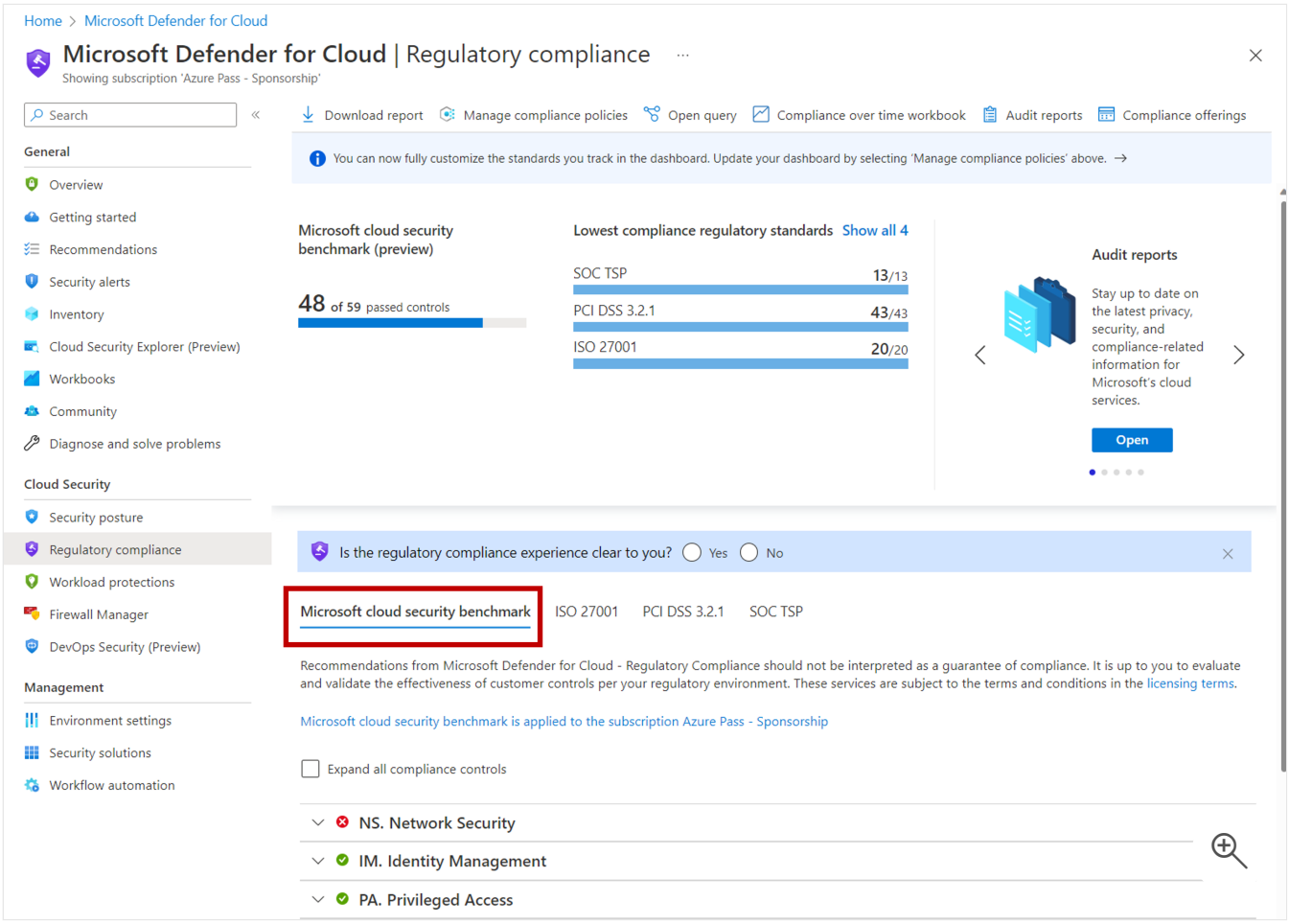
- **Mapping to industry frameworks - The recommendations included in the MCSB map to existing industry frameworks, such as the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standards (PCI DSS) frameworks. This makes security and compliance easier for customer applications running on Azure services.**
- **Recommendation - For each control domain area there can be many distinct recommendations. Each recommendation captures specific functionality associated with the control domain area and is itself a control. For example, the "Network Security" control domain in MCSB v1 has 10 distinct recommendations identified as NS-1 through NS-10. Each of these recommendations describes a specific control under network security. The recommendation identified as NS-1 is to establish network segmentation boundaries.**
- **Security principle - Each recommendation lists a "Security Principle" that explains the "what" for the control at the technology-agnostic level. For the recommendation to establish network segmentation boundaries, one of the points included in the security principle is that any workload that could incur higher risk for the organization should be in isolated virtual networks.**
- **Azure Guidance - Azure Guidance is focused on the "how", elaborating on the relevant technical features and ways to implement the controls in Azure. Continuing with the example of NS-1, the Azure guidance includes information regarding creating a virtual network (VNet), using network security groups (NSG), and using an application security group (ASG).**
- **AWS Guidance - The AWS guidance is focused on the "how" specific to AWS, explaining the AWS technical features and implementation basics.**

The MCSB also includes links to information on implementation that relate to the Azure and AWS guidance, information about security functions at the customer organization who may be accountable, responsible, or consulted for the respective control, and more. The image below is an excerpt from the Microsoft cloud security benchmark version 1 (MCSB v1) and is shown as an example of the type of the content that is included in the MCSB. The image is not intended to show the complete text for any of the line items.

Mapping to industry frameworks

ID	Control Domain	CIS Controls v7.1 ID(s)	CIS Controls v8 ID(s)	NIST SP800-53 r4 ID(s)	PCI-DSS v3.2.1 ID(s)	Recommendation	Security Principle	Azure Guidance	Implementation and additional context	AWS Guidance
NS-1	Network Security	9.2 - Ensure Only Approved Ports, Protocols and Services Are Running 9.4 - Apply Host-Based Firewalls or Port Filtering 12.3 - Deny	3.12 - Segment Data Processing and Storage Based on Sensitivity 13.4 - Perform Traffic Filtering Between Network	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING SC-7: BOUNDARY PROTECTION	1.1 1.2 1.3	Establish network segmentation boundaries	Ensure that your virtual network deployment aligns to your enterprise segmentation strategy defined in the GS-2 security control. Any workload that could incur higher risk for the organization should be in isolated virtual networks.	Create a virtual network (VNet) as a fundamental segmentation approach in your Azure network, so resources such as VMs can be deployed into the VNet within a network boundary. To further segment the network, you can create subnets inside VNet for smaller sub-networks.	Azure Virtual Network concepts and best practices: https://docs.microsoft.com/azure/virtual-network/concepts-and-best-practices Add, change, or delete a virtual network subnet: https://docs.microsoft.com/	Create a Virtual Private Cloud (VPC) as a fundamental segmentation approach in yo AWS network, so resources such as EC2 instances can be deployed into the VPC wit a network boundary. To further segment th network, you can create subnets inside VPC smaller sub-networks. For EC2 instances, use Security Groups, as a
NS-2	Network Security	14.1 - Segment the Network Based on Sensitivity	3.12 - Segment Data Processing and Storage Based on Sensitivity 4.4 - Implement and Manage a	AC-4: INFORMATION FLOW ENFORCEMENT SC-2: APPLICATION PARTITIONING	1.1 1.2 1.3	Secure cloud native services with network controls	Secure cloud services by establishing a private access point for the resources. You should also disable or restrict access from public network when possible.	Deploy private endpoints for all Azure resources that support the Private Link feature, to establish a private access point for the resources. Using Private Link will keep the private connection from routing through the public network.	Understand Azure Private Link: https://docs.microsoft.com/azure/private-link/private-link-overview	Deploy VPC PrivateLink for all AWS resourc that support the PrivateLi 'o allo private connection to th VS services or services hos /S accounts (VPC endpoint s. ng PrivateLink will keep the private connectior from routing through the public network.

Microsoft Defender for Cloud continuously assesses an organization's hybrid cloud environment to analyze the risk factors according to the controls and best practices in the Microsoft cloud security benchmark. Some of the controls used in the MCSB include network security, identity and access control, data protection, data recovery, incident response, and more.



Security baselines for Azure

Security baselines are standardized documents for Azure product offerings, describing the available security capabilities and the optimal security configurations to help you strengthen security through improved tooling, tracking, and security features. Service baselines are currently only available for Azure.

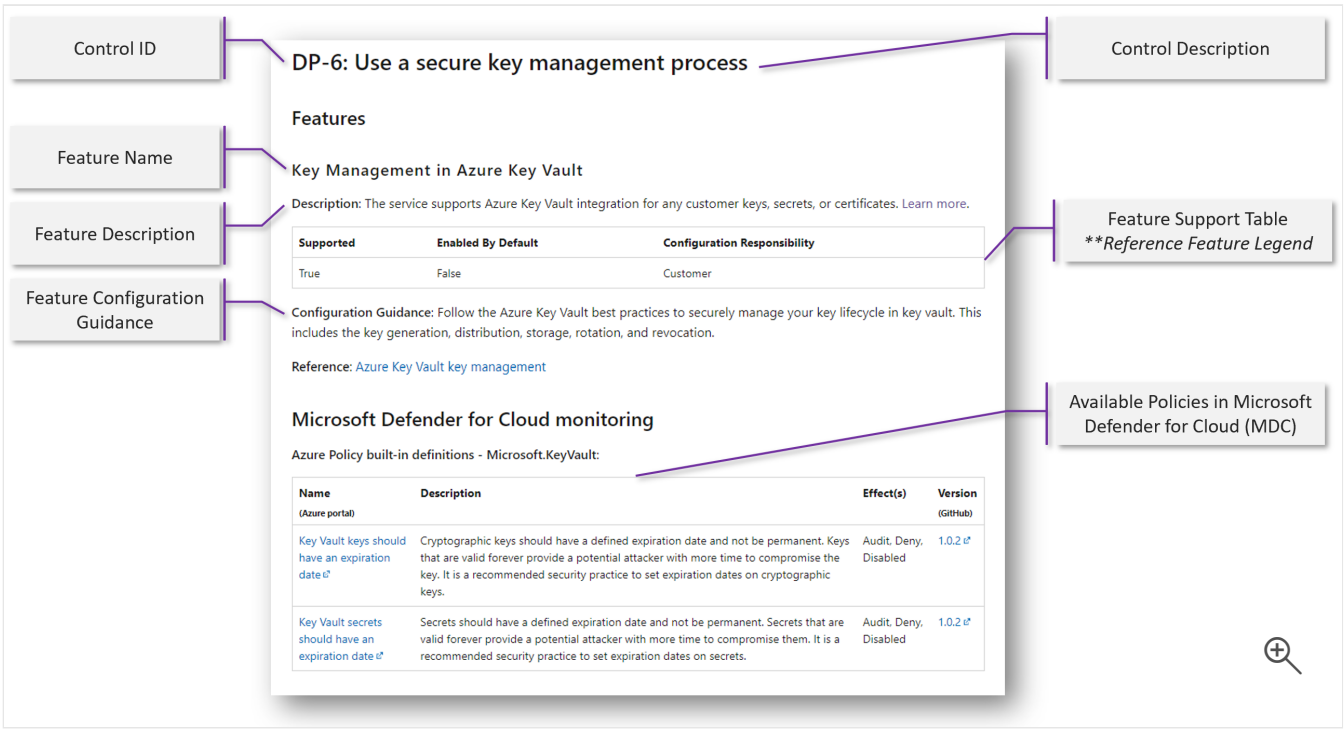
Microsoft cloud security benchmark v1 baselines apply guidance from the Microsoft cloud security benchmark to the specific Azure service for which it's defined. For example, the security baseline for Azure Key Vault applies guidance from the Microsoft cloud security benchmark version 1.0 to Azure Key Vault. Some security baselines may apply guidance from previous benchmarks, such as Azure security benchmark v3.

Content in the security baseline is grouped by the control domains defined by the Microsoft cloud security benchmark that are applicable to the service. A security

baseline includes the following information for each applicable MCSB recommendation (control):

- **Control ID: The Microsoft cloud security benchmark ID that corresponds to the control (recommendation) in the Microsoft cloud security benchmark.**
- **Feature: Security feature(s) that can help you meet that control requirement.**
- **Feature Description: A high-level description of the feature and how it fits into the product offering.**
- **Supported: A true/false value indicating if this feature is supported to secure this product offering.**
- **Enabled by Default: A true/false value indicating if this feature is enabled in a default deployment by Microsoft.**
- **Configuration Responsibility: Who is responsible for implementing the configuration guidance (where possible scenarios are Customer responsibility, Microsoft responsibility or Shared responsibility).**
- **Configuration Guidance: Actionable guidance to implement the configurations.**
- **Microsoft Defender for Cloud monitoring Note: Microsoft Defender for Cloud policy / monitoring information. (Note: If a feature is not monitored by Microsoft Defender for Cloud for the service, this section is omitted.)**
- **Reference: A reference link to dive deeper into how to implement the configuration guidance.**

The image below, which is an excerpt from the Azure Key Vault security baseline, highlights the type of information provided in a security baseline.



Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

Microsoft Azure offers a suite of threat protection and detection systems to minimize and mitigate threats across your whole estate and improve the overall cloud security posture.

You've learned about cloud security posture management (CSPM). You've also explored the capabilities of Microsoft Defender for Cloud and how to understand your security position using secure score. You've discovered the different plans of Microsoft Defender for Cloud that are available and the enhanced security benefits they offer. Finally, you've learned about the Microsoft cloud security benchmark and security baseline in Azure.

Now that you've completed this module, you should be able to:

- **Describe cloud security posture management.**
- **Describe the capabilities of Microsoft Defender for Cloud**
- **Understand the Microsoft cloud security benchmark and security baseline in Azure.**

Learn more

To find out more about any of the topics covered in this module, go to:

- **What is Microsoft Defender for Cloud?**
- **Secure score in Microsoft Defender for Cloud**
- **Microsoft Defender for Cloud pricing**
- **Overview of Microsoft cloud security benchmark (v1)**
- **Security baselines**

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

Every organization, whatever its size, is susceptible to security threats and attacks. Being able to collect data to gain visibility into your digital estate and detect, investigate, and respond to threats is central to any network security strategy.

In this module, you'll learn about the different security defenses that are available to protect your company's digital estate. You'll explore how Microsoft Sentinel provides a single solution for alert detection, threat visibility, proactive hunting, and threat response. Finally, you'll be introduced to Microsoft Security Copilot.

After completing this module, you'll be able to:

- **Describe the security concepts for SIEM and SOAR.**
- **Describe how Microsoft Sentinel provides threat detection and mitigation.**
- **Describe Microsoft Security Copilot.**

Next unit: Define the concepts of SIEM and SOAR

Continue

100 XP

Define the concepts of SIEM and SOAR

1 minute

Protecting an organization's digital estate, resources, assets, and data from security breaches and attacks is an ongoing and escalating challenge. The business world has large numbers of staff working remotely, creating an exploitable window for cybercriminals.

Having a resilient and robust, industry-standard set of tools can help mitigate and prevent these exploits. Security information event management (SIEM) and security orchestration automated response (SOAR) provide security insights and security automation that can enhance an organization's threat visibility and response.

What is security information and event management (SIEM)?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

What is security orchestration automated response (SOAR)?

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

To provide a comprehensive approach to security, an organization needs to use a solution that embraces or combines both SIEM and SOAR functionality.

Next unit: Describe threat detection and mitigation capabilities in Microsoft Sentinel

Continue

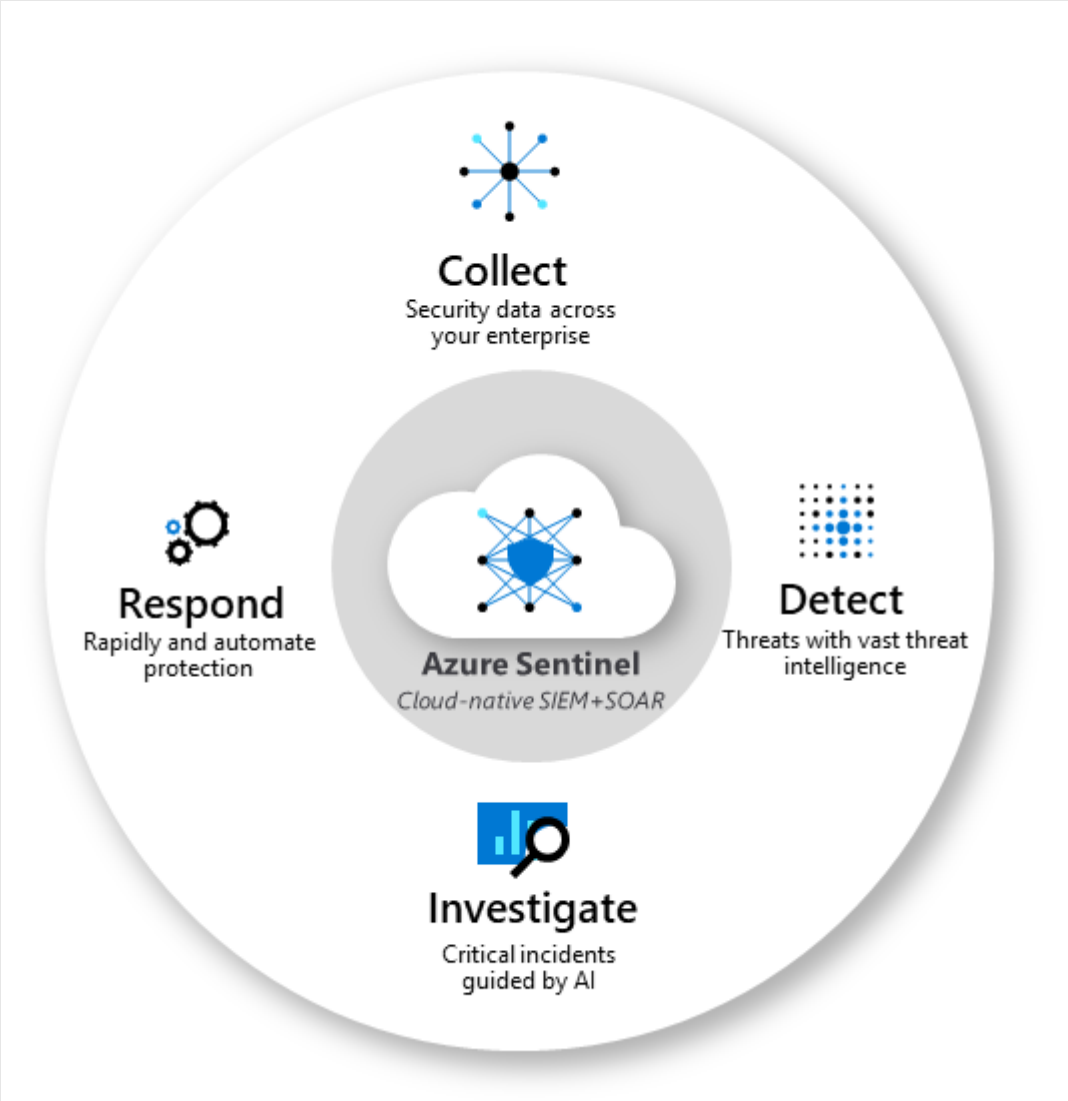
How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe threat detection and mitigation capabilities in Microsoft Sentinel

13 minutes

Effective management of an organization's network security perimeter requires the right combination of tools and systems. Microsoft Sentinel is a scalable, cloud-native SIEM/SOAR solution that delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for alert detection, threat visibility, proactive hunting, and threat response.



This diagram shows the end-to-end functionality of Microsoft Sentinel.

- **Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.**

- **Detect previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence.**
- **Investigate threats with artificial intelligence (AI) and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.**
- **Respond to incidents rapidly with built-in orchestration and automation of common security tasks.**

Microsoft Sentinel helps enable end-to-end security operations, in a modern Security Operations Center (SOC). Listed below are some of the key features of Microsoft Sentinel.

Connect Sentinel to your data

To on-board Microsoft Sentinel, you first need to connect to your security sources. Microsoft Sentinel comes with many connectors for Microsoft solutions, available out of the box and providing real-time integration. Included are Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Microsoft Entra, and more. In addition, there are built-in connectors to the broader security ecosystem of non-Microsoft solutions. You can also connect your data sources using community-built data connectors listed in the Microsoft Sentinel GitHub repository or by following generic deployment procedures for how to connect your data source to Microsoft Sentinel. Links to information are included in the Learn more section of the summary and resources unit.

Workbooks

After you connect data sources to Microsoft Sentinel, you can monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks. Workbooks are intended for SOC engineers and analysts of all tiers to visualize data. You'll see a canvas for data analysis and the creation of rich visual reports within the Azure portal.

Through this integration, Microsoft Sentinel allows you to create custom workbooks across your data. It also comes with built-in workbook templates that allow quick insights across your data as soon as you connect a data source.

Analytics

Microsoft Sentinel uses analytics to correlate alerts into incidents. Incidents are groups of related alerts that together create an actionable possible-threat that you can investigate and resolve. With analytics in Microsoft Sentinel, you can use the built-in correlation rules as-is, or use them as a starting point to build your own. Microsoft

Sentinel also provides machine learning rules to map your network behavior and then look for anomalies across your resources. These analytics connect the dots, by combining low fidelity alerts about different entities into potential high-fidelity security incidents.

Manage incidents in Microsoft Sentinel

Incident management allows you to manage the lifecycle of the incident. View all related alerts that are aggregated into an incident. You can also triage and investigate. Review all related entities in the incident and additional contextual information meaningful to the triage process. Investigate the alerts and related entities to understand the scope of breach. Trigger playbooks on the alerts grouped in the incident to resolve the threat detected by the alert. You can also do standard incident management tasks like changing status or assigning incidents to individuals for investigation.

Security automation and orchestration with playbooks

You can use Microsoft Sentinel to automate some of your security operations and make your security operations center (SOC) more productive. Microsoft Sentinel integrates with Azure Logic Apps, so you can create automated workflows, or playbooks, in response to events. A security playbook is a collection of procedures that can help SOC engineers and analysts of all tiers to automate and simplify tasks and orchestrate a response. Playbooks work best with single, repeatable tasks, and require no coding knowledge.

Investigation

Microsoft Sentinel's deep investigation tools help you to understand the scope of a potential security threat and find the root cause. You choose an entity on the interactive graph to ask specific questions, then drill down into that entity and its connections to get to the root cause of the threat.

Hunting

Use Microsoft Sentinel's powerful hunting search-and-query tools, based on the MITRE framework (a global database of adversary tactics and techniques), to proactively hunt for security threats across your organization’s data sources, before an alert is triggered. After you discover which hunting query provides high-value insights into possible attacks, you can also create custom detection rules based on your query, and surface those insights as alerts to your security incident responders.

While hunting, you can bookmark interesting events. Bookmarking events enables you to return to them later, share them with others, and group them with other correlating events to create a compelling incident for investigation.

Notebooks

Microsoft Sentinel supports Jupyter notebooks. Jupyter Notebook is an open-source web application that allows you to create and share documents that contain live code, equations, visualizations, and narrative text. You can use Jupyter notebooks in Microsoft Sentinel to extend the scope of what you can do with Microsoft Sentinel data. For example, perform analytics that aren't built in to Microsoft Sentinel, such as some Python machine learning features, create data visualizations that aren't built in to Microsoft Sentinel, such as custom timelines and process trees, or integrate data sources outside of Microsoft Sentinel, such as an on-premises data set.

Community

The Microsoft Sentinel community is a powerful resource for threat detection and automation. Microsoft security analysts constantly create and add new workbooks, playbooks, hunting queries, and more, posting them to the community for you to use in your environment. You can download sample content from the private community GitHub repository to create custom workbooks, hunting queries, notebooks, and playbooks for Microsoft Sentinel.

Content hub

The Microsoft Sentinel Content hub is your centralized location to discover and manage out-of-the-box (built-in) packaged solutions. Microsoft Sentinel solutions are packages of Microsoft Sentinel content or Microsoft Sentinel API integrations that provide single-step deployment and enablement. Content hub solutions, which fulfill an end-to-end product, domain, or industry vertical scenario in Microsoft Sentinel.

In the Content hub, filter by categories and other parameters to find the content that works best for your organization's needs and use cases. The Content hub also indicates the support model applied to each solution and content, as some content is maintained by Microsoft and others are maintained by partners or the community. You can also manage updates for out-of-the-box content via the Microsoft Sentinel Content hub.

Next unit: Describe Microsoft Security Copilot

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Security Copilot

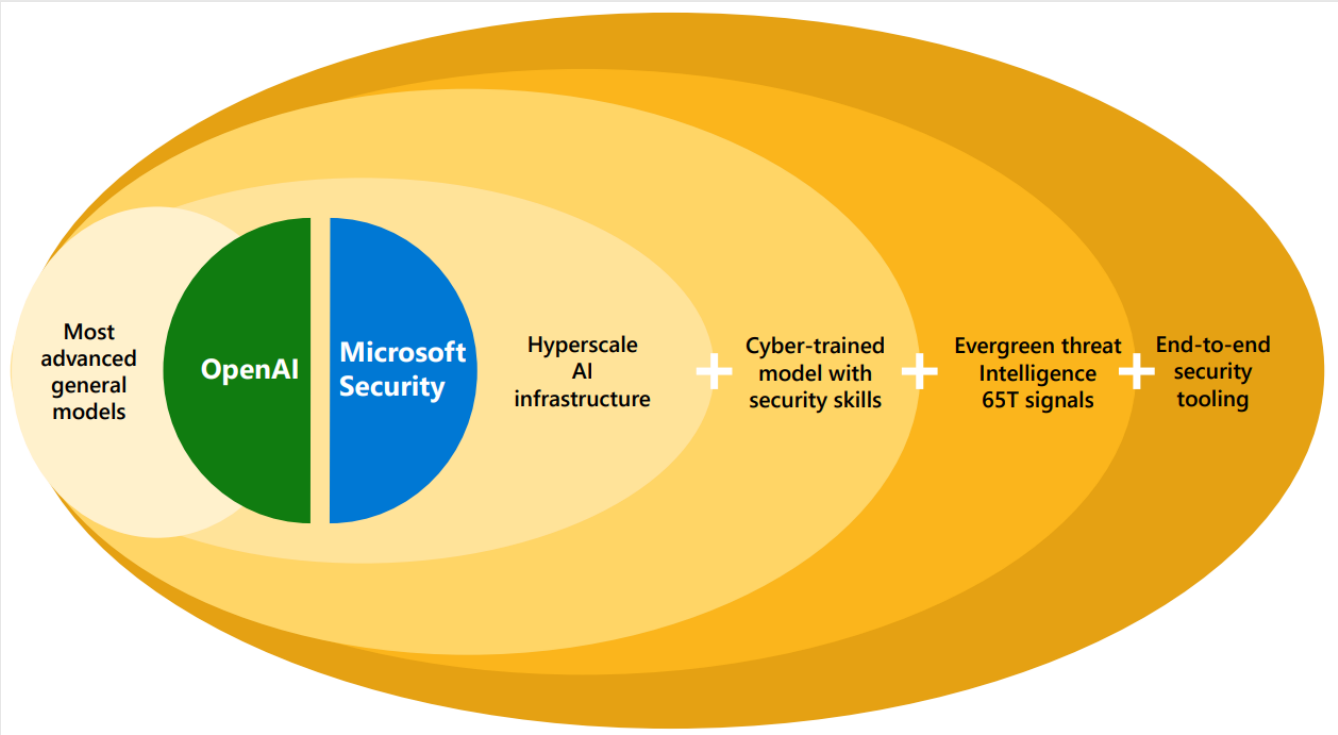
1 minute

The top security challenges organizations face include:

- **An increase in the number and sophistication of attacks.**
- **A talent shortage that is driving the need for automation, integration, and consolidation of security tools.**
- **Visibility into security, privacy, compliance, and governance.**

Organizations need to act quickly to address all the security challenges they face, but working as human speed, even if there weren't a talent shortage, isn't enough. Organizations need to work at machine speed.

Microsoft Security Copilot is the first and only generative AI security product to help defend organizations at machine speed and scale. It's an AI-powered security analysis tool that enables analysts to respond to threats quickly, process signals at machine speed, and assess risk exposure in minutes.



The center of Microsoft Security Copilot is the prompt bar that allows security analysts to ask questions in natural language. You use the prompt bar to tell copilot what insights you want from your security data.

Three primary use cases are security posture management, incident response, and security reporting.

- **Security posture management. Security Copilot delivers information on anything that might expose an organization to a known threat. It then gives the analyst prescriptive guidance on how to protect against those potential vulnerabilities.**
- **Incident response. Security Copilot can quickly surface an incident. For a surfaced incident, Security Copilot can enrich it with context from other data sources, assess its scale and impact, and provide information on what the source might be. Security Copilot can then guide the analyst through the response and remediation steps with guided recommendations. Security Copilot provides single pane of glass visibility by pulling in data from other sources like Defender and Sentinel and then correlating and analyzing that data all together.**
- **Security reporting. Security Copilot can deliver customizable reports that are ready to share and easy to consume, allowing analysts to focus more on high value tasks pertinent for securing the organization.**

The information you give Copilot will only be accessible to your organization. Your data is your data, and it's protected by comprehensive enterprise compliance and security controls. Your data isn't used to train the foundation AI models.

Security Copilot, which is currently in preview and not yet generally available, has planned integration with Microsoft Sentinel and Microsoft's other security product families.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

In this module, you learned about the security defenses available to protect your company's digital estate. You also discovered the key security operation areas that Microsoft Sentinel supports and how it integrates with your existing security systems. You get a single solution for alert detection, threat visibility, proactive hunting, and threat response. You also learned about Microsoft Security Copilot.

Now you've completed this module, you should be able to:

- **Describe the security concepts for SIEM and SOAR.**
- **Describe how Microsoft Sentinel provides threat detection and mitigation.**
- **Describe Microsoft Security Copilot.**

Learn more

To find out more about any of the topics covered in this module, go to:

- **Integrated threat protection with SIEM and XDR**
- **Microsoft Sentinel and SIEM**
- **What is Microsoft Sentinel?**
- **Microsoft Sentinel pricing**
- **Discover and manage Microsoft Sentinel out-of-the-box content**
- **Microsoft Sentinel GitHub repository**
- **Connect your data source,**
- **Introducing Microsoft Security Copilot**

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Introduction

1 minute

Security threat prevention is not limited to just network security. It also covers applications, email, collaborations, endpoints, cross SaaS solutions, identity, and more. With the integrated Microsoft 365 Defender solution, security professionals can stitch together the threat signals that each of these products receive and determine the full scope and impact of the threat; how it entered the environment, what it's affected, and how it's currently impacting the organization.

In this module, you'll learn how Microsoft 365 Defender can help protect your organization. You'll explore each of the different Defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps. You'll also explore the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, reports, and incident management.

After completing this module, you'll be able to:

- **Describe the Microsoft 365 Defender service.**
- **Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.**
- **Describe and explore Microsoft 365 Defender portal.**

Next unit: Describe Microsoft 365 Defender services

Continue

100 XP

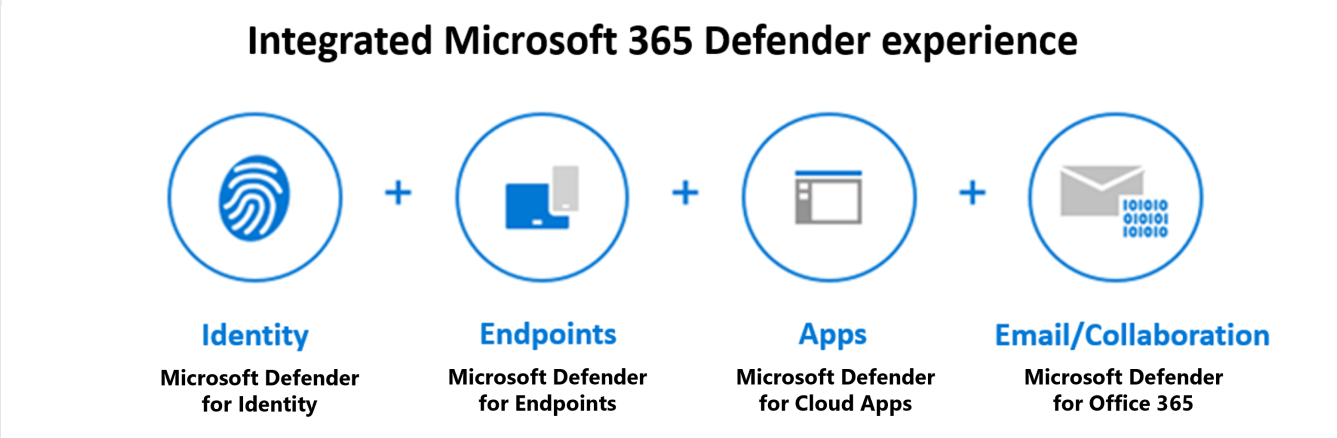
Describe Microsoft 365 Defender services

6 minutes

Microsoft 365 Defender is an enterprise defense suite that protects against sophisticated cyberattacks. With Microsoft 365 Defender, you can natively coordinate the detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications.

This short three-minute video provides an essential overview of Microsoft 365 Defender.

Microsoft 365 Defender allows admins to assess threat signals from endpoints, applications, email, and identities to determine an attack's scope and impact. It gives greater insight into how the threat occurred, and what systems have been affected. Microsoft 365 Defender can then take automated action to prevent or stop the attack.



Microsoft 365 Defender suite protects:

- **Identities with Microsoft Defender for Identity and Azure AD Identity Protection - Microsoft Defender for Identity uses Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.**
- **Endpoints with Microsoft Defender for Endpoint - Microsoft Defender for Endpoint is a unified endpoint platform for preventative protection, post-breach detection, automated investigation, and response.**
- **Applications with Microsoft Defender for Cloud Apps - Microsoft Defender for Cloud Apps is a comprehensive cross-SaaS solution that brings deep visibility, strong data controls, and enhanced threat protection to your cloud apps.**
- **Email and collaboration with Microsoft Defender for Office 365 - Defender for Office 365 safeguards your organization against malicious threats posed by email**

messages, links (URLs), and collaboration tools.

Use Microsoft Defender to protect your organization against sophisticated cyberattacks. It coordinates your detection, prevention, investigation, and response to threats across endpoints, identities, email, and applications.

Next unit: Describe Microsoft Defender for Office 365

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Defender for Office 365

4 minutes

Microsoft Defender for Office 365 safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools, including Microsoft Teams, SharePoint Online, OneDrive for Business, and other Office clients.

Microsoft Defender for Office 365 covers these key areas:

- **Threat protection policies: Define threat protection policies to set the appropriate level of protection for your organization.**
- **Reports: View real-time reports to monitor Microsoft Defender for Office 365 performance in your organization.**
- **Threat investigation and response capabilities: Use leading-edge tools to investigate, understand, simulate, and prevent threats.**
- **Automated investigation and response capabilities: Save time and effort investigating and mitigating threats.**

Microsoft Defender for Office 365 is available in two plans. The plan you choose influences the tools you'll see and use. It's important to make sure you select the best plan to meet your organization's needs.

Microsoft Defender for Office 365 Plan 1

This plan offers configuration, protection, and detection tools for your Office 365 suite:

- **Safe Attachments: Checks email attachments for malicious content.**
- **Safe Links: Links are scanned for each click. A safe link remains accessible, but malicious links are blocked.**
- **Safe Attachments for SharePoint, OneDrive, and Microsoft Teams: Protects your organization when users collaborate and share files by identifying and blocking malicious files in team sites and document libraries.**
- **Anti-phishing protection: Detects attempts to impersonate your users and internal or custom domains.**
- **Real-time detections: A real-time report that allows you to identify and analyze recent threats.**

Microsoft Defender for Office 365 Plan 2

This plan includes all the core features of Plan 1, and provides automation, investigation, remediation, and simulation tools to help protect your Office 365 suite:

- **Threat Trackers: Provide the latest intelligence on prevailing cybersecurity issues, and allow an organization to take countermeasures before there's an actual threat.**
- **Threat Explorer: A real-time report that allows you to identify and analyze recent threats.**
- **Automated investigation and response (AIR): Includes a set of security playbooks that can be launched automatically, such as when an alert is triggered, or manually. A security playbook can start an automated investigation, provide detailed results, and recommend actions that the security team can approve or reject.**
- **Attack Simulator: Allows you to run realistic attack scenarios in your organization to identify vulnerabilities. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.**
- **Proactively hunt for threats with advanced hunting in Microsoft 365 Defender: Advanced hunting is a query-based threat hunting tool that lets you explore up to 30 days of raw data. You can proactively inspect events in your network to locate threat indicators and entities.**
- **Investigate alerts and incidents in Microsoft 365 Defender: Microsoft Defender for Office 365 P2 customers have access to Microsoft 365 Defender integration to efficiently detect, review, and respond to incidents and alerts.**

Microsoft Defender for Office 365 availability

Microsoft Defender for Office 365 is included in certain subscriptions, such as Microsoft 365 E5, Office 365 E5, Office 365 A5, and Microsoft 365 Business Premium.

If your subscription doesn’t include Defender for Office 365, you can purchase it as an add-on.

Use Microsoft Defender for Office 365 to protect your organization's collaboration tools and messages.

Next unit: Describe Microsoft Defender for Endpoint

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

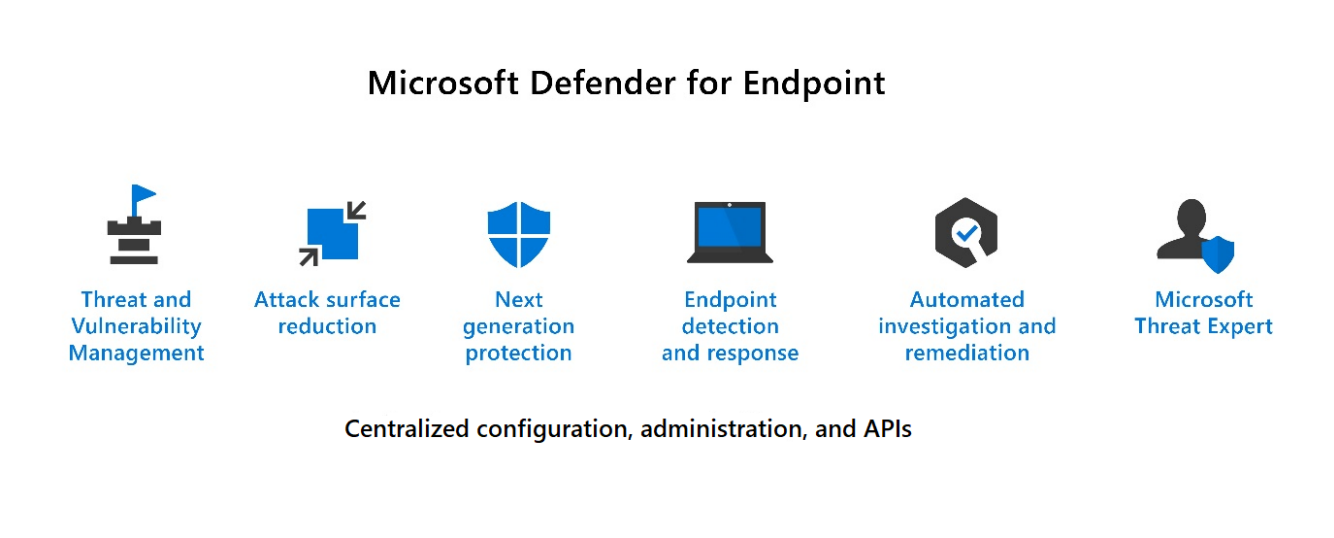
100 XP

Describe Microsoft Defender for Endpoint

3 minutes

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints. It does so by preventing, detecting, investigating, and responding to advanced threats. Microsoft Defender for Endpoint embeds technology built into Windows 10 and Microsoft cloud services.

This technology includes endpoint behavioral sensors that collect and process signals from the operating system, cloud security analytics that turn signals into insights, detections and recommendations, and threat intelligence to identify attacker tools & techniques, and generate alerts.



Microsoft Defender for Endpoint includes:

- **Threat and vulnerability management: A risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. It uses sensors on devices to avoid the need for agents or scans, and prioritizes vulnerabilities.**
- **Attack surface reduction: The attack surface reduction set of capabilities provides the first line of defense in the stack. By ensuring configuration settings are properly set and exploit mitigation techniques are applied, the capabilities resist attacks and exploitation. This set of capabilities also includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URLs; helping prevent apps from accessing dangerous locations**
- **Next generation protection: Brings together machine learning, big data analysis, in-depth threat resistance research, and the Microsoft cloud infrastructure to protect**

devices in your enterprise organization.

- **Endpoint detection and response: Provides advanced attack detections that are near real time and actionable. Security analysts can prioritize alerts, see the full scope of a breach, and take response actions to remediate threats.**
- **Automated investigation and remediation: The automated investigation feature uses inspection algorithms and processes used by analysts (such as playbooks) to examine alerts and take quick remediation action to resolve breaches. This process significantly reduces the volume of alerts that must be investigated individually.**
- **Microsoft Threat Experts: A managed threat hunting service that provides Security Operation Centers (SOCs) with monitoring and analysis tools to ensure critical threats don't get missed.**
- **Management and APIs: Provides APIs to integrate with other solutions.**

Microsoft Defender for Endpoint includes Microsoft Secure Score for Devices to help you dynamically assess the security state of your enterprise network, identify unprotected systems, and take recommended actions to improve overall security. Microsoft Defender for Endpoint integrates with various components in the Microsoft Defender suite, and with other Microsoft solutions including Intune and Microsoft Defender for Cloud.

Use Microsoft Defender for Endpoint to protect your organization's endpoints and respond to advanced threats.

Next unit: Describe Microsoft Defender for Cloud Apps

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Defender for Cloud Apps

11 minutes

Moving to the cloud increases flexibility for employees and IT teams. However, it also introduces new challenges and complexities for keeping your organization secure. To get the full benefit of cloud apps and services, an IT team must find the right balance for supporting access while protecting critical data.

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB). It's a comprehensive cross-SaaS solution that operates as an intermediary between a cloud user and the cloud provider. Microsoft Defender for Cloud Apps provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services. Use this service to gain visibility into Shadow IT by discovering the cloud apps being used. You can control and protect data in the apps after you sanction them to the service.

What is a Cloud Access Security Broker?

A CASB acts as a gatekeeper to broker real-time access between your enterprise users and the cloud resources they use, wherever they're located, and regardless of the device they're using. CASBs help organizations protect their environment by providing a wide range of capabilities across the following pillars:

- **Visibility - Detect cloud services and app use and provide visibility into Shadow IT.**
- **Threat protection - Monitor user activities for anomalous behaviors, control access to resources through access controls, and mitigate malware.**
- **Data security - Identify, classify and control sensitive information, protecting against malicious actors.**
- **Compliance - Assess the compliance of cloud services.**

These capability areas represent the basis of the Defender for Cloud Apps framework described below.

The Defender for Cloud Apps framework

Microsoft Defender for Cloud Apps is built on a framework that provides the following capabilities:

- **Discover and control the use of Shadow IT: Identify the cloud apps, and IaaS and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks.**
- **Protect against cyberthreats and anomalies: Detect unusual behavior across cloud apps to identify ransomware, compromised users, or rogue applications, analyze high-risk usage, and remediate automatically to limit risks.**
- **Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Use out-of-the-box policies and automated processes to apply controls in real time across all your cloud apps.**
- **Assess your cloud apps' compliance: Assess if your cloud apps meet relevant compliance requirements, including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps and limit access to regulated data.**

Microsoft Defender for Cloud Apps functionality

Defender for Cloud Apps Security delivers on the components of the framework through an extensive list of features and functionality. Listed below are some examples.

- **Cloud Discovery maps and identifies your cloud environment and the cloud apps your organization uses. Cloud Discovery uses your traffic logs to dynamically discover and analyze the cloud apps being used.**

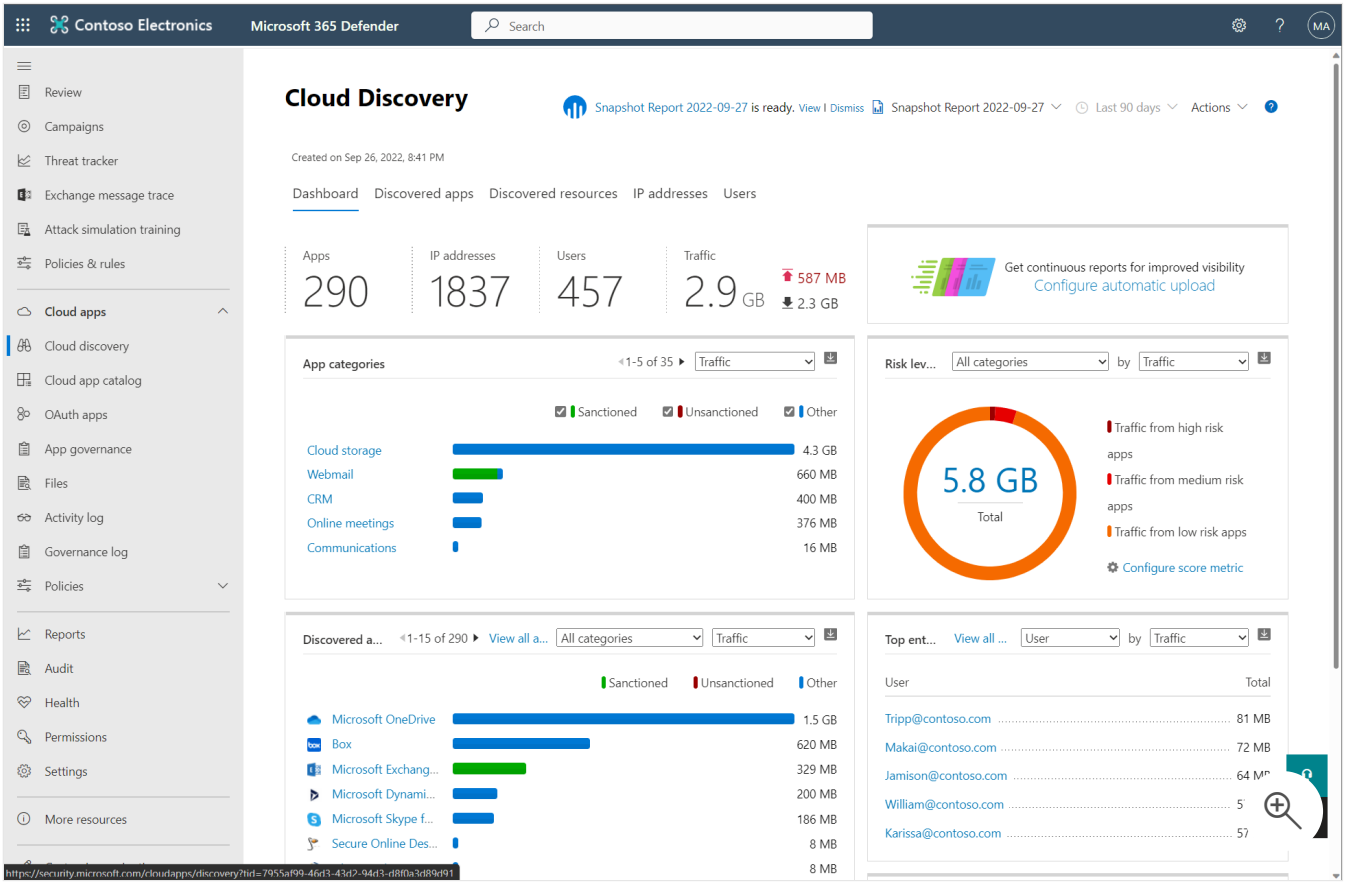
- **Sanctioning and unsanctioning apps in your organization by using the Cloud apps catalog that includes over 25,000 cloud apps. The apps are ranked and scored based on industry standards. You can use the cloud app catalog to rate the risk for your cloud apps based on regulatory certifications, industry standards, and best practices.**

- **Use App connectors to integrate Microsoft and non-Microsoft cloud apps with Microsoft Defender for Cloud Apps, extending control and protection. Defender for Cloud Apps queries the app for activity logs, and it scans data, accounts, and cloud content that can be used to enforce policies, detect threats and provide governance actions to resolve issues.**

- **Conditional Access App Control protection provides real-time visibility and control over access and activities within your cloud apps. Avoid data leaks by blocking downloads before they happen, setting rules to require data stored in and**

downloaded from the cloud to be protected with encryption, and controlling access from non-corporate or risky networks.

- **Use policies to detect risky behavior, violations, or suspicious data points and activities in your cloud environment. You can use policies to integrate remediation processes to achieve risk mitigation.**



In this interactive guide, you'll get an introduction to the capabilities available with Microsoft Defender for Cloud Apps. Select the image below to get started and follow the prompts on the screen.

Office 365 Cloud App Security

Office 365 Cloud App Security is a subset of Microsoft Defender for Cloud Apps that provides enhanced visibility and control for Office 365. Office 365 Cloud App Security includes threat detection based on user activity logs, discovery of Shadow IT for apps with similar functionality to Office 365 offerings, control app permissions to Office 365, and apply access and session controls.

It offers a subset of the core Microsoft Defender for Cloud Apps features.

Enhanced Cloud App Discovery in Azure Active Directory

Azure Active Directory Premium P1 includes Azure Active Directory Cloud App Discovery at no extra cost. This feature is based on the Microsoft Defender for Cloud Apps Cloud Discovery capabilities that provide deeper visibility into cloud app usage in your organization.

It provides a reduced subset of the Microsoft Defender for Cloud Apps discovery capabilities.

Use Microsoft Defender for Cloud Apps to intelligently and proactively identify and respond to threats across your organization's Microsoft and non-Microsoft cloud services.

Next unit: Describe Microsoft Defender for Identity

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe Microsoft Defender for Identity

3 minutes

Microsoft Defender for Identity is a cloud-based security solution. It uses your on-premises Active Directory data (called signals) to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Microsoft Defender for Identity provides security professionals managing hybrid environments functionality to:

- **Monitor and profile user behavior and activities.**
- **Protect user identities and reduce the attack surface.**
- **Identify and investigate suspicious activities and advanced attacks across the cyberattack kill-chain.**
- **Provide clear incident information on a simple timeline for fast triage**

Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user. Defender for Identity then identifies anomalies with adaptive built-in intelligence. It gives insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.

Protect user identities and reduce the attack surface

Defender for Identity provides insights on identity configurations and suggested security best practices. Through security reports and user profile analytics, Defender for Identity helps reduce your organizational attack surface, making it harder to compromise user credentials and advance an attack.

Defender for Identity security reports, help identify users and devices that authenticate using clear-text passwords. It also provides extra insights into how to improve security posture and policies.

For hybrid environments in which Active Directory Federation Services (AD FS) is present, Defender for Identity protects the AD FS by detecting on-premises attacks and

providing visibility into authentication events generated by the AD FS.

Identify suspicious activities and advanced attacks across the cyberattack kill-chain

Typically, attacks are launched against any accessible entity, such as a low-privileged user. Attacks then quickly move laterally until the attacker accesses valuable assets. These assets might include sensitive accounts, domain administrators, and highly sensitive data. Defender for Identity identifies these advanced threats at the source throughout the entire cyberattack kill-chain:

- **Reconnaissance**
- **Compromised credentials**
- **Lateral movements**
- **Domain dominance**

Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Use the Defender for Identity attack timeline view and the intelligence of smart analytics to stay focused on what matters. Also, you can use Defender for Identity to quickly investigate threats, and gain insights across the organization for users, devices, and network resources.

Microsoft Defender for Identity protects your organization from compromised identities, advanced threats, and malicious insider actions.

Next unit: Describe the Microsoft 365 Defender portal

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Describe the Microsoft 365 Defender portal

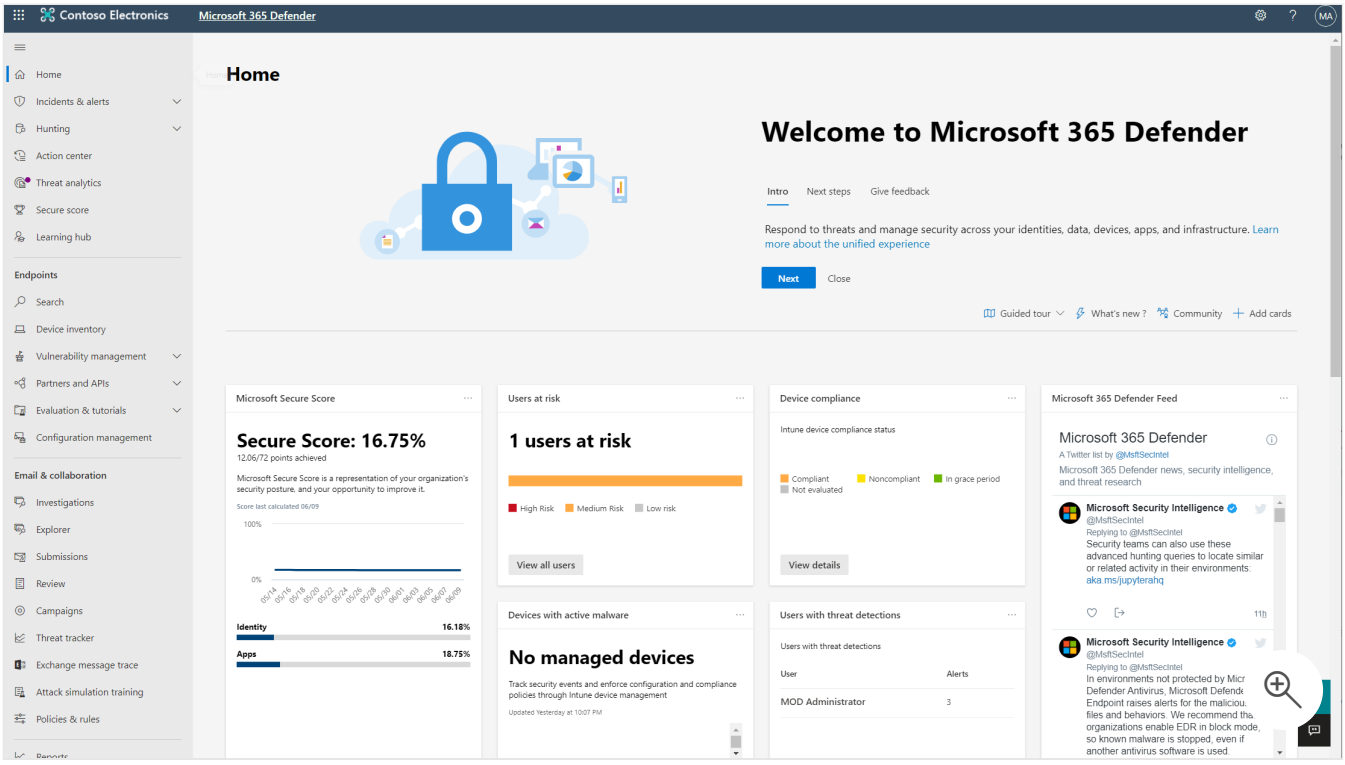
10 minutes

Microsoft 365 Defender natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. The Microsoft 365 Defender portal brings this functionality together into a central place that is designed to meet the needs of security teams and emphasizes quick access to information, simpler layouts. Through the Microsoft 365 Defender portal you can view the security health of your organization.

The Microsoft 365 Defender portal home page shows many of the common cards that security teams need. The composition of cards and data depends on the user role. Because the Microsoft 365 Defender portal uses role-based access control, different roles will see cards that are more meaningful to their day-to-day jobs.

The cards fall into these categories:

- **Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors.**
- **Data - Help track user activity that could lead to unauthorized data disclosure.**
- **Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.**
- **Apps - Gain insight into how cloud apps are being used in your organization.**



The Microsoft 365 Defender portal allows admins to tailor the navigation pane to meet daily operational needs. Admins can customize the navigation pane to show or hide functions and services based on their specific preferences. Customization is specific to the individual admin, so other admins won't see these changes.

> **Note**
>
> **You must be assigned an appropriate role, such as Global Administrator, Security Administrator, Security Operator, or Security Reader in Azure Active Directory to access the Microsoft 365 Defender portal.**

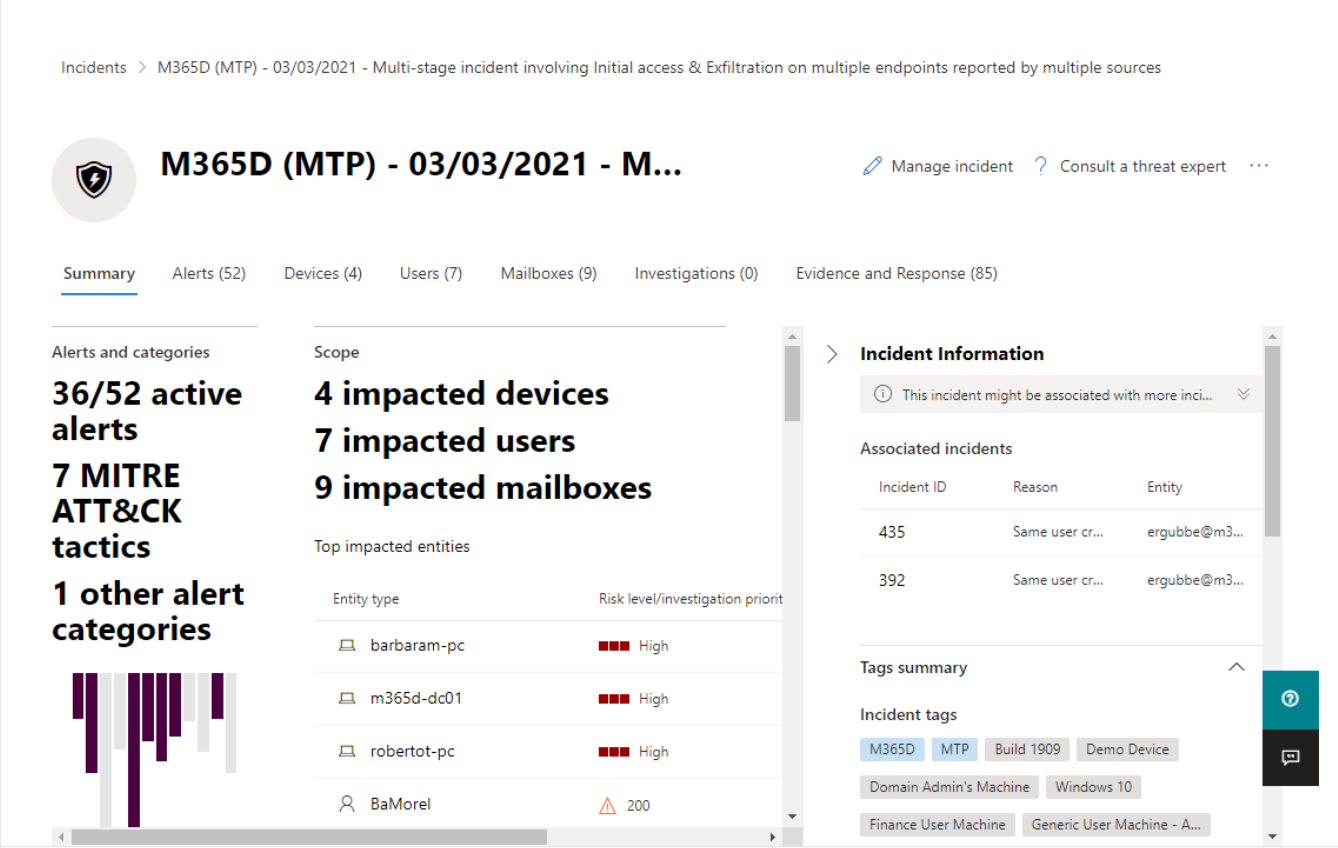
The left navigation pane provides security professionals easy access to the email and collaboration capabilities of Microsoft Defender for Office 365 and the capabilities for Microsoft Defender for Endpoint which were described in the previous units. Listed below we describe a few of the other capabilities accessible from the left navigation bar in the Microsoft 365 Defender portal.

Incidents and alerts

Microsoft 365 services and apps create alerts when they detect a suspicious or malicious event or activity. Individual alerts provide valuable clues about a completed or ongoing attack. These alerts are automatically aggregated by Microsoft 365 Defender. It's the grouping of these related alerts that form an incident. The incident provides a comprehensive view and context of an attack.

The incidents queue is a central location lists each incident by severity. Selecting an incident name displays a summary of the incident and provides access to tabs with additional information, including:

- **All the alerts related to the incident.**
- **All the users that have been identified to be part of or related to the incident.**
- **All the mailboxes that have been identified to be part of or related to the incident.**
- **All the automated investigations triggered by the alerts in the incident.**
- **All the supported evidence and response.**



Hunting

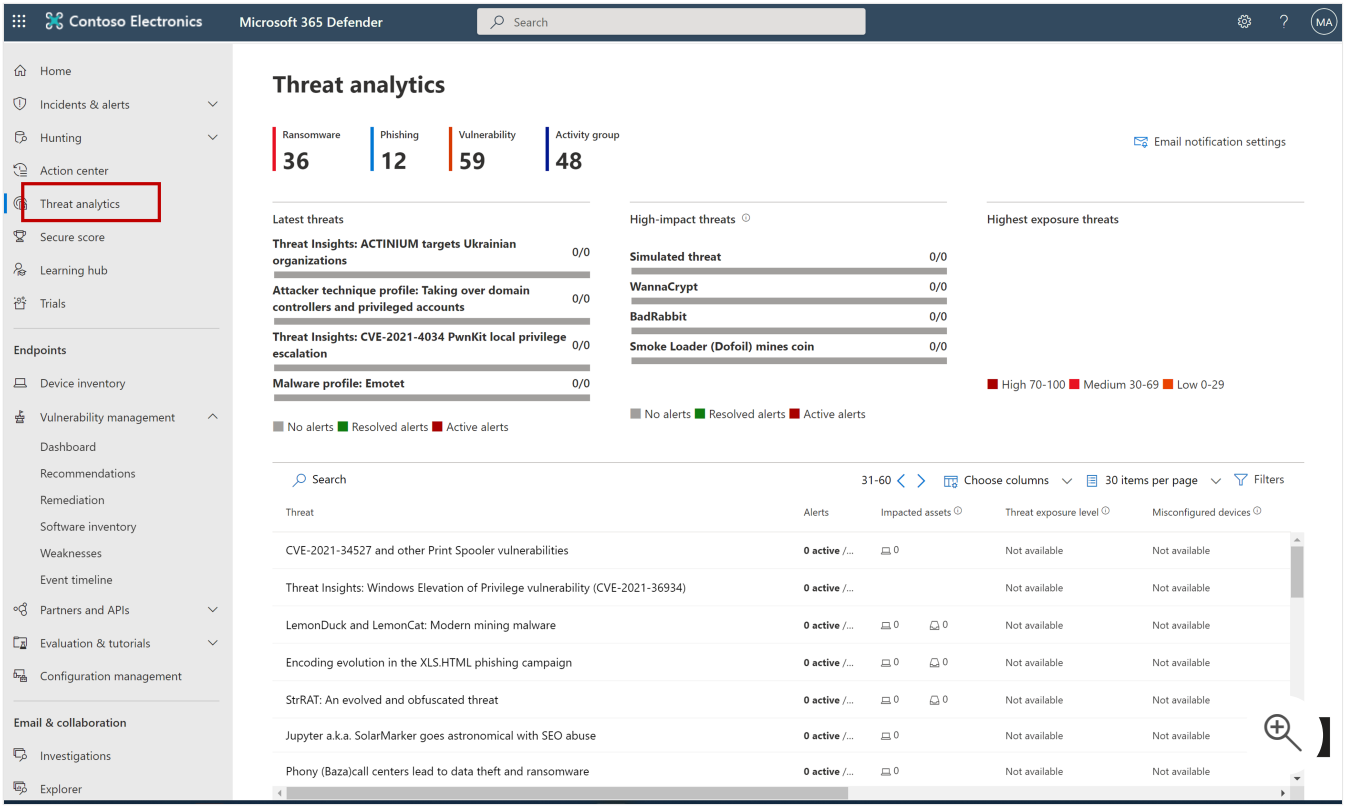
Advanced hunting is a query-based threat-hunting tool that lets security professionals explore up to 30 days of raw data. Advanced hunting queries enable security professionals to proactively search for threats, malware, and malicious activity across your endpoints, Office 365 mailboxes, and more. Threat-hunting queries can be used to build custom detection rules. These rules run automatically to check for and then respond to suspected breach activity, misconfigured machines, and other findings.

Threat analytics

Threat analytics is our in-product threat intelligence solution from expert Microsoft security researchers. It's designed to assist security teams track and respond to emerging

threats. The threat analytics dashboard highlights the reports that are most relevant to your organization. It includes the latest threats, high impact threats (threats with the most active alerts affecting your organization), and high exposure threats.

Selecting a specific threat from the dashboard provides a threat analytics report that provides more detailed information that includes detailed analyst report, impacted assets, mitigations, and much more.



Secure Score

Microsoft Secure Score, one of the tools in the Microsoft 365 Defender portal, is a representation of a company's security posture. The higher the score, the better your protection. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

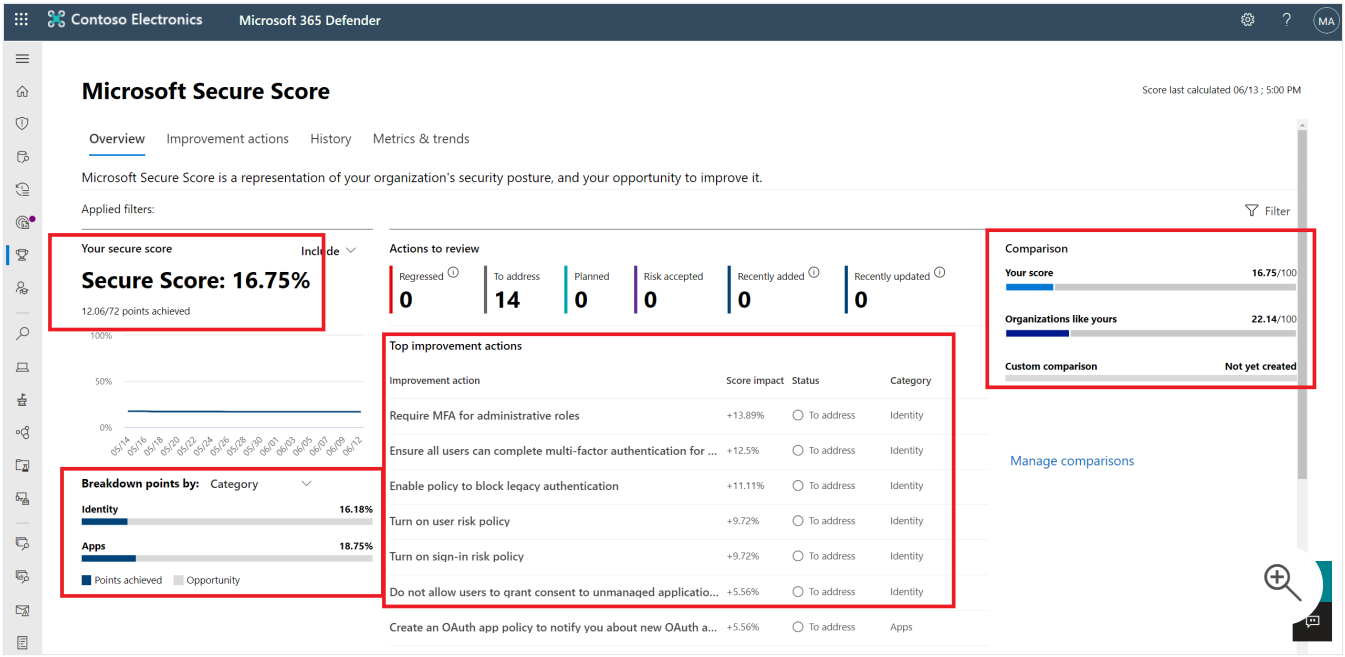
Secure Score helps organizations:

- **Report on the current state of their security posture.**
- **Improve their security posture by providing discoverability, visibility, guidance, and control.**
- **Compare benchmarks and establish key performance indicators (KPIs).**

Currently Microsoft Secure Score supports recommendations for Microsoft 365 (including Exchange Online), Azure Active Directory, Microsoft Defender for Endpoint,

Microsoft Defender for Identity, Microsoft Defender Cloud Apps, and Microsoft Teams. New recommendations are being added to Secure Score all the time.

The image below shows an organization's Secure Score, a breakdown of the score by points, and the improvement actions that can boost the organization's score. Finally, it provides an indication of how well the organization's Secure Score compares to other similar organizations.



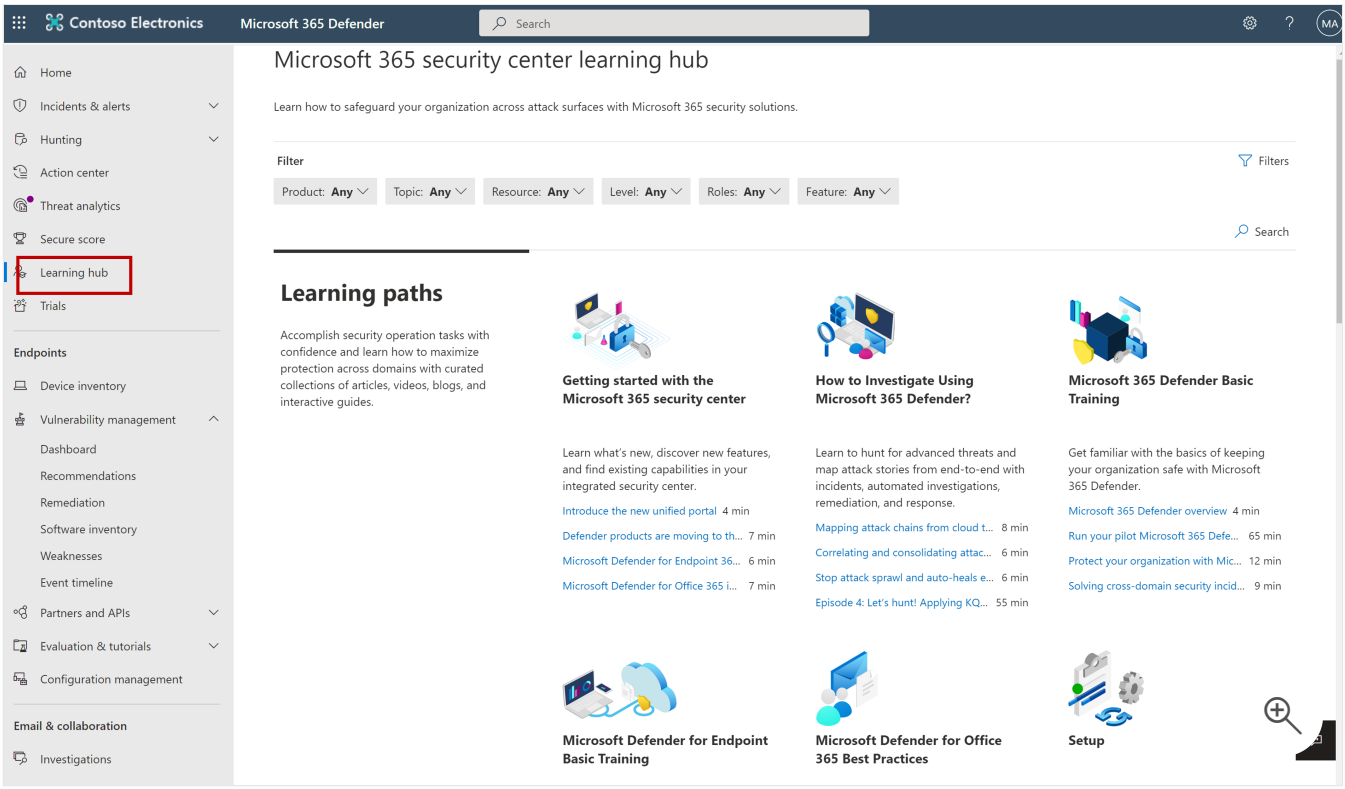
To explore Microsoft Secure Score, select the interactive guide below and follow the prompts on the screen.

Differences between secure score in Microsoft 365 Defender and Microsoft Defender for Cloud

There's a secure score for both Microsoft 365 Defender and Microsoft Defender for Cloud, but they're subtly different. Secure score in Microsoft Defender for Cloud is a measure of the security posture of your Azure subscriptions. Secure score in the Microsoft 365 Defender portal is a measure of the security posture of the organization across your apps, devices, and identities.

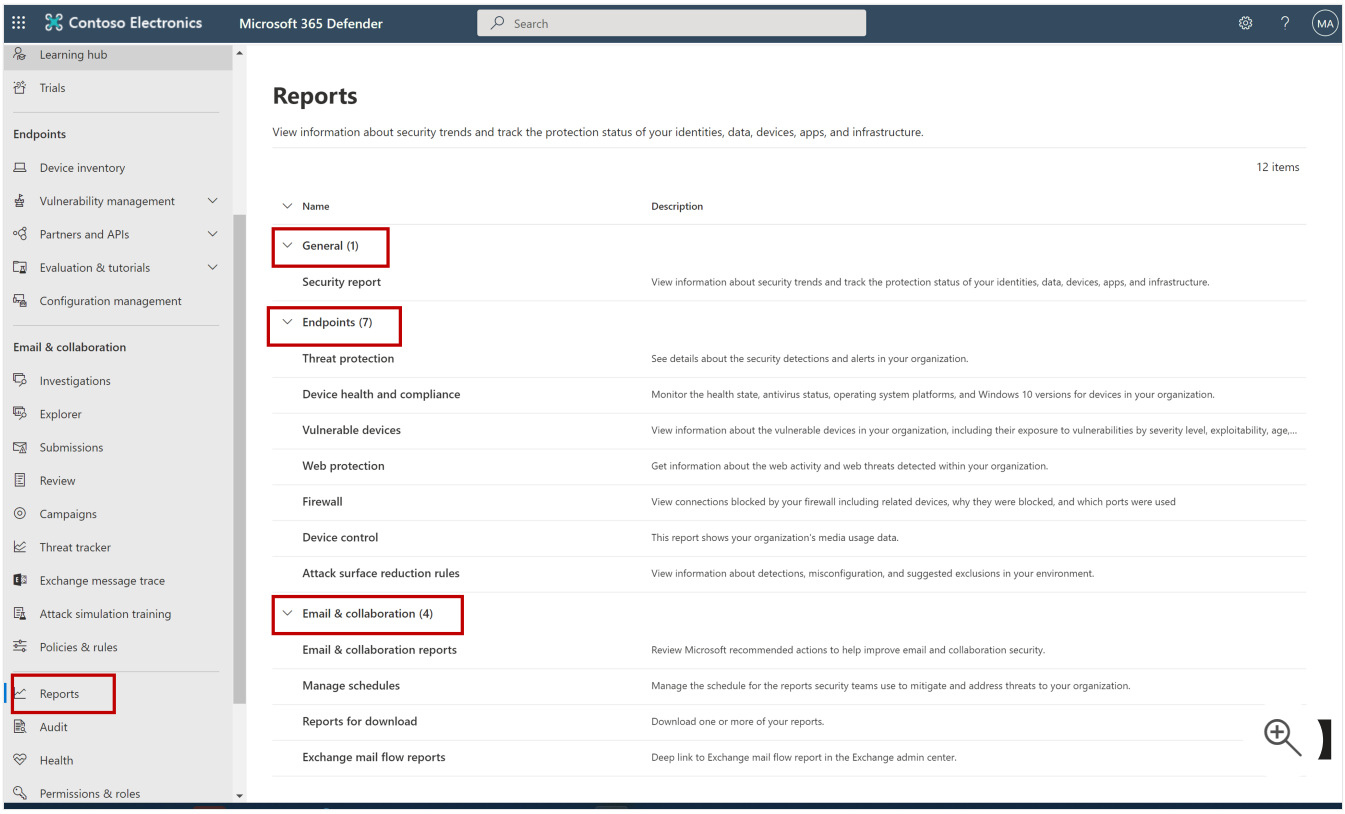
Learning hub

The Microsoft 365 Defender portal includes a learning hub that bubbles up official guidance from resources such as the Microsoft security blog, the Microsoft security community on YouTube, and the official documentation on Microsoft Learn.



Reports

Reports are unified in Microsoft 365 Defender. Admins can start with a general security report, and branch into specific reports about endpoints, email & collaboration. The links here are dynamically generated based upon workload configuration.



Permissions & roles

Access to Microsoft 365 Defender is configured with Azure Active Directory global roles or by using custom roles.

Next unit: Knowledge check

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆

100 XP

Summary and resources

1 minute

In this module, you learned how Microsoft 365 Defender can help protect your organization. You explored each of the different Defender services to understand how they can protect: Identity, Office 365, Endpoint, and cloud apps. You also explored the capabilities of the Microsoft 365 Defender portal, including Microsoft Secure Score, reports, and incident management.

Now you've completed this module, you'll be able to:

- **Describe the Microsoft 365 Defender service.**
- **Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks.**
- **Describe and explore Microsoft 365 Defender portal.**

Learn more

To find out more about any of the topics covered in this module, please visit these links:

- Microsoft 365 Defender
- Microsoft Defender for Identity
- Microsoft Defender for Office 365
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud Apps
- Overview of the Microsoft 365 Defender portal
- Incident response with Microsoft 365 Defender
- Threat analytics in Microsoft 365 Defender
- Microsoft Secure Score
- Integrated reports
- Incidents overview in Microsoft 365 Defender

Module complete:

Unlock achievement

How are we doing? ☆ ☆ ☆ ☆ ☆